



CYBERSECURITY

INSIDE: Market highlights · Deal volumes · Key players · About Clairfield



JOSEPH SABET
SECTOR HEAD

WHAT'S NEW IN THE SECURITY SOFTWARE SECTOR

COVID-19 has driven radical change in businesses. As offices are empty, employees are adapting to the new mode of working from home. The COVID-19 pandemic has forced enterprises to rapidly adapt to new working models. Companies are looking to connect reliably, scale rapidly, and stay protected as today's workforces need ways to communicate and collaborate as they transition from on-premise to remote working. Although the coronavirus has had an impact in M&A activity across the board, interest in cybersecurity is rising as it becomes ever more indispensable. After a record year in 2019 in terms of both volume and value of deals, cybersecurity remains one of the clear hot sectors for the future as well.

According to Cyber Security Ventures global spending on cybersecurity will exceed USD 1 trillion cumulatively over the five-year period of 2017 to 2021. With 35X growth many start-ups have entered the market. As the market becomes crowded, consolidation will follow. Startups often have more advanced R&D and are acquired by larger companies who need to move quickly to protect their dominant market position. Further consolidation will make it more challenging for niche security vendors to compete, especially since large-cap companies offer end-to-end solutions and are viewed by enterprises as a "one-stop-shop".

2019 was a strong year for capital markets, and cybersecurity stocks outperformed both the S&P 500 and NASDAQ. These stocks go up whenever there are hacks of big name companies. In the past year Facebook, Disney, Macy's, and Capital One were some of the many enterprises whose customer data was compromised as a result of cyber-attacks.

In 2019 188 deals were completed with venture financing in excess of USD 100 million. Within the sector, security services lead M&A with MSSPs and cyber consulting firms as the most sought after companies. Such companies will likely need to acquire tech-enabled add-ons with recurring revenues to differentiate their offering as the sector matures.

We have noted the following M&A trends:

- 27% of deals were PE related. 73% strategic, mostly publicly traded.
- Private equity has been funding growth equity rather than taking controlling positions.
- Service companies have become active acquirors, taking advantage of business preference to outsource network monitoring to service companies rather than to buy their own software with constant updates required. Companies offering such services have been the most interesting targets. E&Y, for example, has become an active acquiror, joining these cybersecurity companies to its consulting practice.
- The size of financing deals size is increasing. There were 21 financings in excess of USD 100 million last year. Traditional PE funds have turned into growth capital investors that seek to accelerate development and market penetration in order to have a first-to-market mover advantage. The most active sector for investment was Risk & Compliance.



TRENDS IN CYBERSECURITY



Cloud backup of critical systems is necessary to ensure business continuity, especially in work-from-home situations. Leading organizations are investing in cloud security as it becomes the mainstream computing platform. Until recently data stored in cloud applications like O365, GSuite, Box, Dropbox, and Salesforce was thought to be secure. In reality the data stored in such SaaS applications has not been invulnerable. Cloud backup services are increasingly popular and inexpensive security solutions.



Hackers have quickly adapted their email phishing techniques by exploiting fears of COVID-19 with emails on health updates, fake cures, fiscal packages, emergency benefits, and supply shortages. Becoming a victim of a phishing attack is common at even sophisticated organizations. Many businesses acknowledge that payment of ransomware after an attack despite government warnings not to do so. More organizations are turning to cyber insurance to protect their assets and uptime. We expect to see a significant increase in the number of entities buying cyber insurance, making it one of the fastest growing markets related to cyber security.



We see further development of cybersecurity solutions that leverage artificial intelligence (AI) and machine learning (ML) to dynamically identify threats in real-time so that organizations can act proactively rather than reactively to threats. AI and ML are used to understand patterns, threat detection, automate, and respond to cyber security processes and facilitate decision-making.



Passwords have long been a vulnerability in the security chain. More organizations are gravitating towards next-generation authentication technologies, such as biometrics and multi-factor authentication.



The human element is the weakest link in cybersecurity. Over 30% of breaches are carried out by insiders. Many companies are implementing privileged access solutions to prevent employees from obtaining access to files or transferring data out of the enterprise. The Zero Trust approach to access management threat prevention has been gaining traction.



As 5G networks roll out, the use of connected IoT devices will accelerate dramatically, massively increasing network vulnerability to large scale, multi-vector 5th generation cyberattacks. IoT devices and their connections to networks and clouds are still a weak link in security.



Mobile banking malware is on the rise. Payment data, credentials, and funds can be accessed by cybercriminals with as little as an unwary click on the user's mobile device. Consumers are swindled into handing over their personal data through their most common means of communications, including email, SMS texting attack, social media posts, and gaming platforms. These attacks are expected to intensify.



Since the launch of GDPR in Europe, similar data protection laws have been adopted by the state of California, Australia, Brazil and Canada, to name a few. New regulations have led enterprises to increase their cybersecurity budget to meet these requirements.



CYBERSECURITY M&A TRANSACTIONS

Most of the transactions in the first half of 2020 were in the process of being sold prior to breakout of Covid-19 and include the following:

TARGET	ACQUIROR	EV (USD million)
 ARMIS.	 INSIGHT PARTNERS	1,100
 f5	 SH-PE	1,000
 Checkmarx	 HELLMAN & FRIEDMAN	1,150
 CLOUDGENIX	 paloalto NETWORKS	420
 Contact Info Security	 accenture	132

2019 M&A TRANSACTIONS

TARGET	ACQUIROR	EV (USD million)
 Symantec.	 BROADCOM.	10,700
 SOPHOS	 THOMA BRAVO	3,948
 Carbon Black.	 vmware®	2,100
 SH-PE	 f5	1,000
 KeyW	 Jacobs	815
 Recorded Future	 INSIGHT PARTNERS	780
 WEBROOT	 CARBONITE	618,5
 Secure Link	 orange™	577
 DEMISTO	 paloalto NETWORKS	560



CYBERSECURITY M&A OVERVIEW 2019

TRANSACTIONS



MOST ACTIVE STRATEGIC BUYERS

BUYER	No. of deals
paloalto NETWORKS	5
Akamai	3
Check Point SOFTWARE TECHNOLOGIES LTD	3
SOPHOS	3
EY	3

LEADING PRIVATE EQUITY CYBERSECURITY TRANSACTIONS

TARGET	PE INVESTOR	USD million
SOPHOS	THOMA BRAVO	3,948
VERACODE	THOMA BRAVO	950
Centrify	THOMA BRAVO	500
LogRhythm	THOMA BRAVO	535

LEADING M&A CONSOLIDATORS



CYBERSECURITY IPO'S



OTHER LEADING PE CONSOLIDATORS





CYBERSECURITY DEAL SPOTLIGHT

France/Dubai

Boss Industries

acquired



SOFTWARE & APPS

Boss Industries, a French group dedicated to homeland security solutions, acquired Trovicor.

Based in Dubai, Trovicor is a leading provider of turnkey end-to-end lawful interception and intelligence solutions. It targets law enforcement, public safety, and government intelligence communities in the fight against drug trafficking, cyber money laundering, human trafficking, terrorism, and other criminal activities.

RECENT CLAIRFIELD TRANSACTIONS

United States



merged with



SECURITY COMPLIANCE SOLUTIONS

United States



acquired



IDENTITY VERIFICATION

Australia/United States



acquired



CYBER DEFENCE

United States



issued Convertible Preferred Stock to an investor group led by



SOFTWARE & APPS

France



sold



to



IT SECURITY SERVICES

Canada



WV CORPORATION

raised funds from



INFORMATION SECURITY

Luxembourg/France

Fairness opinion

for



DATA IDENTITY AND DATA SECURITY

Netherlands

Management and



acquired



IT SECURITY SOLUTIONS



CLOAK AND DAGGER FOR THE DIGITAL AGE

Q&A WITH STEPHANE SALIES



Stephane Salies is founder and CEO of Boss Industries, a growing cyber intelligence group including Nexa Technologies.

What is cyber intelligence exactly, and what does Boss Industries do? Are your clients in law enforcement or are there business and private clients?

Cyber intelligence consists of using software and hardware systems to intercept, gather, analyze, and interpret data, be it voice, internet use, social network postings, or any other communication, in order to identify, qualify, and report threats and crimes to government intelligence and law enforcement agencies. It is an essential tool for homeland security today when physical barriers no longer exist.

Is cyber intelligence an international business?

Cyber intelligence is now critical for every single country in the world on a nationwide level, but it is also used to protect groups of people, such as military forces, wherever they are deployed. It is indeed a very international business. Some countries use their own proprietary technologies, for example the NSA in the US, but most countries buy and utilize the most advanced solutions regardless of the nation of origin. The main players are originally Israeli, American, or European, among which a few companies, considered the best technology providers, dominate the market. Some of the well-known players include Verint (listed on NASDAQ, USD 3 billion in market cap), NSO Group (Israel, bought and re-sold by Francisco Partners), BAE Systems (UK), Rohde Schwarz (Germany), and Thales (France). These firms are our competitors in tenders and also constitute a good benchmark in terms of value creation and recognition by financial investors.

What are the strategic considerations of these companies? Are there special issues in the M&A process due to the sensitive nature of the work?

Technological innovation is vital. Coping with fast moving data and communication systems is a key success factor. Geopolitically speaking, being a European player is a key success factor as it allows to work in all geographical areas except embargoed countries such as North Korea and Iran, or the US, China, and Russia. The M&A process is indeed special given the confidentiality owed to clients but also because not all companies can be sold to any buyer.

We are celebrating Clairfield’s 15th year in 2020. What has changed in cyber intelligence in the last 15-20 years?

Twenty years ago, cyber intelligence was basically telephone voice interception. In 20 years, IP communication has developed exponentially. It became imperative to be able to address the new technologies.

At the same time, terrorism developed on a global scale, not limited by borders, as September 11th tragically demonstrated. In this context, new players have appeared and developed quickly in a kind of wild-west in the data world versus analog communications. As the industry continued to grow, all players and governments understood the strategic importance of such systems and clients became more aware and educated about which providers they could securely buy products from.

What is your relationship to Clairfield?

Clairfield Paris has been our advisor for the last 15 years, assisting us in all M&A transactions that we consider, including sales, strategic partnerships, and acquisitions, including two acquisitions in 2019. The team knows and understands our business and is committed as a long-term partner. Clairfield’s international capability is key.

300+

TEAM MEMBERS

30%

DEALS CLOSED WITH INTERNATIONAL BUYES

400

NUMBER OF ACTIVE CROSSBORDER CLIENTS

CLAIRFIELD INTERNATIONAL

23

COUNTRY TEAMS ACROSS THE WORLD

130+

DEALS CLOSED ANNUALLY

EUR 20 billion

CUMULATIVE DEAL VALUE LAST 5 YEARS

Clairfield International was founded in 2004 by four European M&A boutiques and has since expanded to encompass all major economies worldwide with the addition of knowledgeable partners in key markets.

Our strengths are our entrepreneurial spirit, local expertise, industry know-how, and close bonds among all team members spanning the globe.



Leading independent M&A advisor for midmarket deals

Top 10

IN EUROPEAN MIDMARKET RANKINGS

Top 20

IN WORLDWIDE MIDMARKET RANKINGS

80%

OF OUR MANDATES ARE INTERNATIONAL

1100+

ANNUAL ASSIGNMENTS ON BEHALF OF CORPORATES, INVESTORS AND FAMILY BUSINESSES

Contact:

Joseph Sabet

Head of Cybersecurity practice
jsabet@clairfield.com
T: +972 3 607-4100

Bertrand Hermez

Head of TMT sector group
bhermez@clairfield.com
T: +33 1 40 20 12 34

Thierry Chetrit

CEO, France
tchetrit@clairfield.com
T: +33 1 40 20 12 34

Clairfield International SA
11 Rue du Conseil-Général
1205 Geneva, Switzerland
Tel: +41 22 518 024
info@clairfield.com

www.clairfield.com

DISCLAIMER: No part of this report may be reproduced without the written permission of Clairfield International. The information herein has been obtained from sources that we believe to be reliable, but we do not guarantee its accuracy or completeness. Much of the information contained in this report is subject to variation due to changes in market conditions, legislation or regulatory matters and Clairfield International does not undertake to notify any recipient of the report of changes to the information contained herein. This report is not to be construed as an offer to sell or the solicitation of an offer to buy any security in any jurisdiction. Additional supporting information is available upon request. Contact: Press office, Clairfield International, Tel: +41 22 518 0242, press@clairfield.com