START-UP NATION CENTRAL: FINDER INSIGHTS SERIES
ISRAEL’S CYBERSECURITY INDUSTRY IN 2016
EXECUTIVE SUMMARY

In 2016, Israel’s Cybersecurity sector maintained its leading position as a global center of innovation. It continued its long-term growth and set a record for capital raised, with a total of $581 million in investments in 2016, a 9 percent increase from 2015. This sum represents 15 percent of the total venture capital raised by cybersecurity companies throughout the world.

Other statistics from 2016 demonstrate the growing maturity of the Israeli Cybersecurity industry, with series A round investments averaging 44 percent higher than in 2015 and accounting for most of the total transaction volume.

Of the 65 start-ups founded in 2016, 25 percent have already successfully raised a series A round or seed funding, with an average investment of $1.6 million. 2016 witnessed slightly fewer exits than in 2015, which may actually be evidence of maturity in the sector, possibly reflecting a change in shareholders’ goals; instead of seeking acquisitions in early stages, they may now be more prepared to wait to reach growth and maturity stages before exiting.

Data leaks, breaches, and cybercrime continued to make headlines in 2016 following some of the most extensive cyberattacks and data breaches ever documented. Reports on state-sponsored attacks have become more common, while more digital and physical assets were found to be susceptible to attack, such as critical infrastructure, mobile phones and IoT devices. Ransomware became an even more popular and harmful method of attack than the year before and has become more sophisticated and accessible to hackers.

During 2016, Israel’s Cybersecurity industry made considerable efforts to meet the challenges posed by the growing threat of cyberattacks. The OT (operational technology) and ICS (industrial control systems) subsector, which deals with threats to SCADA and critical infrastructure, had a very successful year, with four companies raising a total of $55 million in impressive investment rounds.

Cybersecurity companies providing security solutions for IoT devices and connected cars also experienced accelerated growth in 2016, with nineteen companies currently active in that field.
The year 2016 will be remembered as a turbulent one for cybersecurity, with cyber-related incidents dominating headlines and demonstrating the great vulnerability of so many aspects of modern life. The year began with the disruption of the electricity supply in western Ukraine, the first known successful cyberattack on a power grid. Even the American presidential elections were influenced by a massive leak of email correspondence between Hillary Clinton and Democratic National Committee members. In addition, the infrastructure of the financial sector once again proved vulnerable when $81 million were stolen from the central bank of Bangladesh in just a few hours through the SWIFT global payment network, with only a small typo exposing the anomalous transactions and preventing the attackers from stealing up to $1 billion. Another notable attack occurred in October when Dyn, a DNS (domain name service) provider, experienced multiple DDOS (distributed denial of service) attacks, which shut down major Internet services, including Amazon, Twitter and Spotify. The attack was executed by hacking a massive number of connected devices, such as home routers, closed circuit cameras and baby monitors.

Many data breach incidents also made headlines. Yahoo! announced two occurrences, one of which constituted the largest data breach ever documented, affecting over one billion accounts that included phone numbers, full names, hashed passwords, and security questions, all stolen in mid-2013 and discovered only in 2016. No sector is immune, as TrapX Security has shown that healthcare services have become increasingly prone to breaches in personal healthcare data. In 2016, the number of data breaches in healthcare institutions in the United States increased by 63 percent.1

Among the incidents that made headlines in the last year, ransomware continues to be a leading threat to all industries.2 The security company Kaspersky Lab reports that businesses became victims of crypto-ransomware three times more frequently in 2016 than in the preceding year and that the attacks have become more sophisticated.3 Such phenomena are likely to continue in 2017, possibly through the ever-growing use of ransomware-as-a-service. New methods and targets of attack can also be expected, such as shutting down manufacturing and production lines and compromising IoT devices.

The fight against cybercrime becomes more difficult as the sophistication and frequency of attacks increase. Attackers can be private, as in the case of the Yahoo! data breach, or state-sponsored, as alleged by the global press in the cases of the American presidential campaign and the western Ukrainian electricity grid. Attacks can be motivated by monetary incentives, as with the Bangladesh bank heist, or by political, terrorist or activist objectives. Defense against these attacks requires constant collaboration among policymakers, defense agencies, private cybersecurity companies and the vulnerable targets. Israel, with its dynamic Cybersecurity industry strengthened by government support and initiatives, plays a significant role in the global efforts to attain cybersecurity.

**ISRAEL’S CYBERSECURITY SECTOR**

With demand for innovative cybersecurity solutions growing, Israel’s Cybersecurity sector maintains its position as a global leader. There are currently 365 cybersecurity companies active in Israel, 65 of which were founded in 2016, compared to 60 in 2015. In 2016, Israel’s Cybersecurity sector broke its own record for financing raised, reaching $581 million in investments, second only to the United States and representing 15 percent of the capital raised by the global Cybersecurity industry that year.4 The presence of multinational corporations in Israel has expanded, including Huawei’s acquisition of Hexatier and Volkswagen’s founding of CyMotive Technologies to provide security solutions for connected cars.

---

4 Figures based on Start-Up Nation Finder and PitchBook.
FUNDRAISING

As discussed earlier, total investments in 2016 reached $581 million, a record for the Israeli Cybersecurity sector, exceeding 2015 investments by 9 percent, despite the fact that the number of funding rounds decreased by 7 percent, from 67 to 62. Although 2016 was a record-breaking year for fundraising, the last quarter registered the lowest level of VC (venture capital) activity since the end of 2014 (see Charts 2 and 4). This trend in Israel resembles global VC activity during the last quarter of 2016.\(^5\)

The composition of different funding series reveals major changes during the past year. While there were fewer seed rounds, the number of series A rounds rose to an unprecedented total of 32 (see Chart 3). The decrease in the number of seed rounds can be attributed to a number of factors, including the increasing simplicity of the validation process through innovation hubs and design partners, which enables early-stage start-ups to skip seed rounds.

In addition to the increase in the number of series A funding rounds, their average size may also serve as an indicator of the maturity of Israel’s Cybersecurity sector. The average funding round size in 2016 amounted to $9.3 million, up from 2015’s $8 million. The average series A round size grew by an impressive 44 percent from the previous year, from $6.3 million in 2015 to $9.1 million in 2016. This growth is attributed to some major transactions, among them $32 million raised by Claroty, $30 million raised by Cato Networks and $20 million raised by FireGlass.

Of the 65 companies founded in 2016, 25 percent already raised their seed funding during the year, a number comparable to that of the cybersecurity companies founded in 2015. Widening our scope, we can see that over 60 percent of the companies founded since the beginning of 2015 have already achieved at least one financing round, which is a very high rate compared to other sectors in the Israeli economy, where the average is only 21 percent.

The year 2016 entailed considerable involvement of corporates and corporate venture capital funds (CVCs) in cybersecurity investment. Thirty-five percent of 2016’s funding rounds were led by corporates or CVCs, a significant increase of 25 percent from 2015 and of 21 percent since 2014. Among them were Deutsche Telekom Capital Partners, which invested in SafeBreach and FireGlass, and Singtel Innov8, which invested in Cato Networks and FireGlass. Another CVC that was very active in Israeli cybersecurity in the past year was Rafael Development Corporation (RDC), the commercialization arm of Rafael Advanced Defense Systems, and its early-stage VC fund, RDSeed. Angel investors contributed over $170 million to funding rounds in 2016, amounting to over 34 percent of all funding rounds in Israeli cybersecurity companies. Shlomo Kramer was the most active angel investor, investing in more than six companies, among them: TopSpin, Aqua Security, and Indegy.

EXITS

The number and volume of exit transactions in the Cybersecurity sector fell in 2016, consistent with the overall decrease in the number of exits by Israeli companies throughout the high-tech industry. There were thirteen exits in the Cybersecurity sector worth over $600 million in total, representing a reduction of 25 percent in number and 52 percent in value from the previous year. The average exit amounted to $51 million, compared to $80 million in 2015. The largest exits in 2016 were Cisco Systems’ acquisition of CloudLock for $293 million, Providence Strategic Growth’s buyout of Skybox Security for $96 million and Harman International Industries’ acquisition of the automotive cybersecurity company, TowerSec, for $75 million.

The predominant exit method was M&A, utilized in seven, or 60 percent, of all exits. As in 2015, no cybersecurity company held an IPO. The companies Safe-T and Genome Technologies held a reverse merger and became public.

In light of the decrease in the number of M&As (notwithstanding the increase in the average size of both early- and late-stage funding rounds) it appears that more and more cybersecurity companies prefer to take their time to grow before seeking an exit rather than being acquired for smaller amounts at earlier stages of development. Therefore, we expect the decline in the number of M&As to be only temporary. The reduction of Israeli IPOs coincides with the global decrease in IPOs in 2015 and most of 2016. Still, in accordance with TechCrunch’s forecast regarding IPOs worldwide in 2017, and based on early predictions, we anticipate additional IPOs by Israeli cybersecurity companies in the coming year.

---

6 See e.g. Shira Ovide, “This Year’s Tech IPO Crop Stunts Next One”, Bloomberg (November 2016); Sandy Miller, “The Drought is Over.. A Torrent of Tech IPOs is Expected in 2017”, TechCrunch (December 2016).

7 Ibid.
SUBSECTORS

The largest Cybersecurity subsectors in terms of absolute number of active companies are Network Security (67), Anti-fraud and Authentication (48) and Data Protection (41).

Between 2015 and 2016, the IoT and Automotive Security sector grew significantly, with fourteen companies founded. In contrast, the number of Anti-fraud and Authentication companies being founded since 2014 has been falling, with only eleven founded between 2015 and 2016, compared to 25 between 2013 and 2014.

With regard to fundraising, the subsectors Network Security, Anti-fraud and Authentication and Mobile Security received the most funding. In contrast, in 2015, nearly half the capital raised went to End-point Security and to Secure Coding as the result of two considerably large funding rounds: Checkmarx with $84 million and Cybersean with $59 million.

The OT/ICS security subsector, which protects OT, SCADA, critical infrastructure networks and industrial control systems, had a very dynamic year, with four investments totaling $55 million. Among them were Team8’s company, Claroty, which raised $32 million, Indegy, which raised $12 million and CyberX, which raised $9 million, all carried out in Q3. Threat Intelligence companies also enjoyed a successful year, with IntSights and SixGill raising $75 million and $5 million respectively in series A rounds.

Companies offering solutions for security operations experienced considerable growth, with seven companies raising $43 million in 2016, compared to 2015, when five companies raised only $13 million. This subsector’s success in 2016 is due to a shortage of analysts for SOC (Security Operations Center) teams and the need for automation of security operations in areas such as analytics, incident response and forensics. Investment in End-point security decreased, with only four investments totaling $29 million, compared to nine investments worth $127 million in total during 2015.

8 This subsector differentiation is being used for the purposes of this report only. Some companies actually fall into more than one subsector and classification can vary over time.
EVENTS AND CONFERENCES

Israel hosts some of the most influential international cybersecurity conferences, attended by world leaders, key players in the industry, academics and tech experts. Cybertech, ICRC’s Cyber Week, Team8’s Rethink Cyber, and Israel Cyber & HLS are just a few examples of events that attracted thousands of visitors from Israel and abroad in 2016.

In the pipeline for 2017:

**The Israeli Delegation to the RSA Conference, hosted by the Israeli Economic Mission and the Israeli Export Institute**

(February 13–16, San Francisco)

**ISDEF**

June 6–8, Tel Aviv

This year is dedicated to the Cybersecurity and Fintech sectors (June 6–8, Tel Aviv)

**CyberWeek**

June 25th–29th, 2017

Held by Blavatnik Interdisciplinary Cyber Research Center (ICRC) and the Yuval Ne’eman Workshop for Science, Technology, and Security (June 25–29, Israel)

ABOUT START-UP NATION CENTRAL

Start-Up Nation Central is a not-for-profit, completely neutral and non-conflicted organization that promotes Israeli innovation. Start-Up Nation Central connects companies and countries to the people and technologies in Israel that can solve their most pressing challenges. We are the authoritative source on, and the GPS to, the Israeli innovation community. We provide international clients with their first tangible point of connection to the Israeli innovation ecosystem by designing highly customized engagements for government and business leaders, acquainting them directly with the innovation they need. We also created the largest and most up-to-date free platform for data and connectivity to more than 5,000 Israeli companies, as well as investors, and multinational corporations operating in Israel.

AUTHORS

Nir Falevich: Analyst, Cybersecurity Sector Lead, Nir.falevich@sncentral.org

CONTACT

For more information on the companies cited in this report and the Israeli Cybersecurity sector in general, please visit finder.startupnationcentral.org.

Questions and comments should be directed to Shmuel Rausnitz (shmuel.rausnitz@sncentral.org).

APPENDIX: METHODOLOGY

Data Set: Figures regarding the Israeli Cybersecurity sector are based entirely on Start-Up Nation Finder™, a free online platform that maps Israel’s innovative companies. Start-Up Nation Central defines an “Israeli innovative company” as an entity founded in Israel. Companies that have moved overseas are excluded from the platform unless they maintain a substantial presence in Israel, including R&D. The platform does not include service providers.

Fundraising: This refers to any equity transaction, such as VC or angel investments, or private equity in the growth stage, excluding majority liquidity, which is considered a buyout (see Exits). Fundraising amounts refer only to the value invested in a given year, even if an agreement includes terms for potential future obligations, these figures are not included in this report.

Exits: This refers only to first-time full or major liquidity events of companies that have not been previously acquired, including M&As, buyouts, reverse mergers and IPOs.