Deloitte.

Israel Cyber Industry Overview

Deloitte Corporate Finance Israel

March 2024

Table of Contents

Executive Summary

Deloitte Israel’s Corporate Finance and Cyber Risk Service practices conducted a joint analysis on Israel’s cyber industry to identify recent trends and shifts and the current state of the Israeli cyber industry today, as well as to analyze of what may be happening in 2024-2025.

In contrast to various tech sectors, the Israeli cybersecurity industry showcases the most pronounced correlation with global trends. Amidst the broader challenges faced by the Israeli tech ecosystem in regaining momentum post the global downturn of 2021-2022, cybersecurity emerges as a pivotal domain displaying robust indications of recovery. Even in the face of escalating geopolitical challenges, the cybersecurity sector persists in demonstrating resilience and ongoing progress. However, many cyber companies that secured capital during the peak of 2021 and early 2022 might encounter a divergence between their last round’s valuation and the current valuation that new investors would be willing to apply.

Leveraging public data sources such as financial data providers alongside press news, articles, and industry reports, Deloitte Israel uncovered the following crucial insights:

1. M&A activity among Israeli cyber companies is projected to surge this upcoming year (2024-2025).

2. We expect the trend of local consolidation among Israel's cyber companies, witnessed initially during 2023, to further intensify.

3. Growth stage companies, with $10m-$30m revenues, represent nearly 20% of the companies we mapped. 70% of these companies had their last round in the peak times of 2021-2022. These companies may need to raise capital soon and the ones with lower growth rates could be reluctant to raise at a down-round valuation.

The following comprehensive analyses, unveils and elaborates on these findings, this analysis may to empower stakeholders to capitalize on the projected increase in cybersecurity M&A activities and the growing trend of local consolidation.

.91
13716.02
16248.27

H

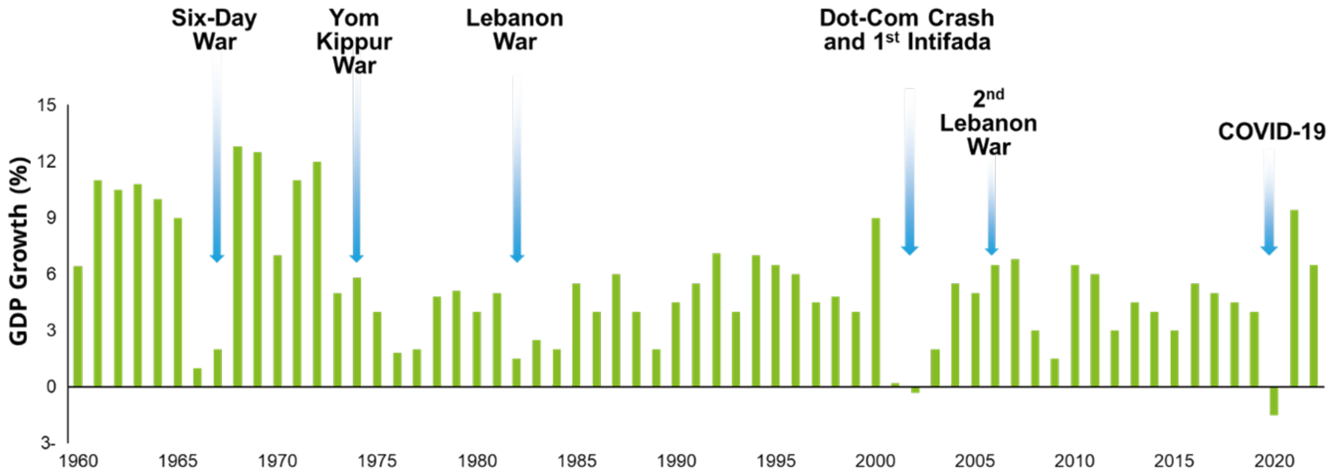
Key Trends and Insights

Tech Ecosystem Shaping Forces

Deloitte Israel has conducted research, covering global and local recent events and their potential effects on the Israeli economy and on the tech ecosystem [1].
One cannot predict the outcomes of the current local geopolitical situation and discern the complete implications of the ongoing war.

Nonetheless, by drawing insights from past events with similar characteristics, it may be reasonable to anticipate a medium-term recovery that will counterbalance the immediate short-term impact. However, it's worth noting that during those prior instances, the Israeli economy was not as globally interconnected as it stands today.

Past events and implications on GDP:

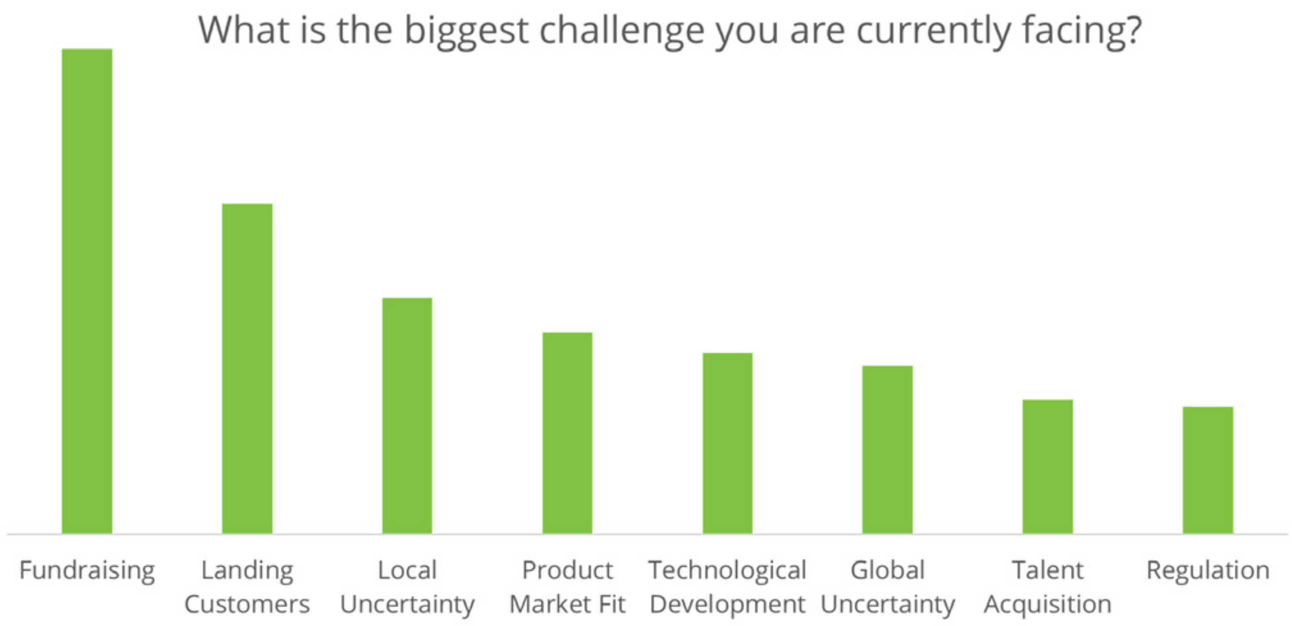


Source: "Macro Economic Trends and Update Growth Expectations for 2023-2024", Israel Ministry of Finance (November 2023)

Throughout our research, we have pinpointed various influential forces that could shape the tech ecosystem in the upcoming years.:

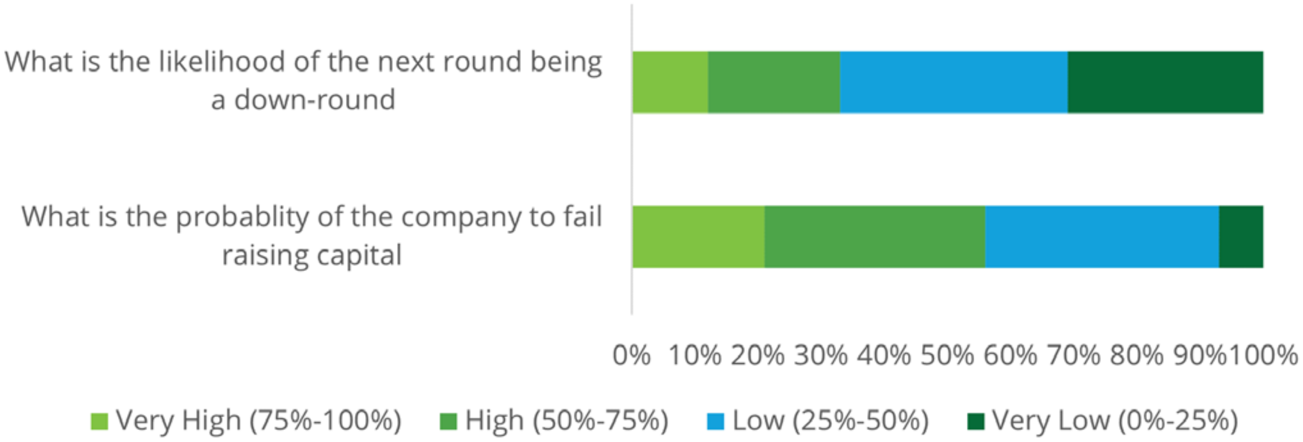
- The impact on the entire tech ecosystem may be felt in three dimensions:
  a. Financing innovation
  b. Positioning and competitiveness compared with global markets
  c. Talent acquisition
- Potential impact on capital raising may be stronger on early-stage companies.

Among the challenges companies are facing, Fundraising was the most significant one companies' management mentioned they are facing:



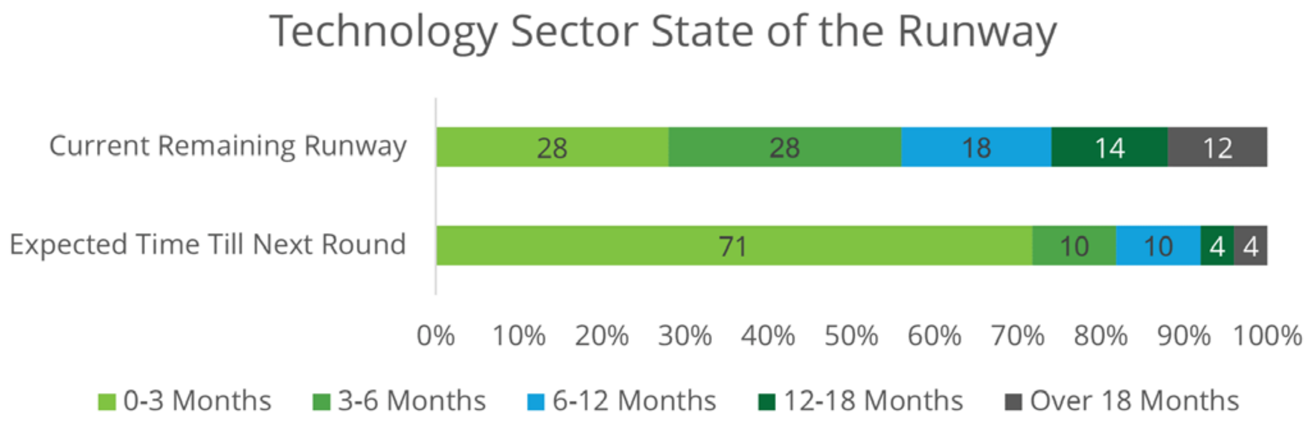
Source: "Iron Swords, Point of View", Deloitte Monitor Israel (December 2023)

These conclusions are also coherent with the Israel Innovation Authority's survey from December 2023 [(2)], emphasizing the challenge of raising capital. In this survey, 56% of responders believe there is a high probability of them failing to raise their next round of capital. Additionally, 33% of responders believe that their next round is expected to be a down-round.



Source: "Companies' Survey", Israel Innovation Authority (December 2023)

These estimations are set to materialize imminently, given that 76% of respondents have a runway of less than a year, and over 90% anticipate raising capital in 2024.

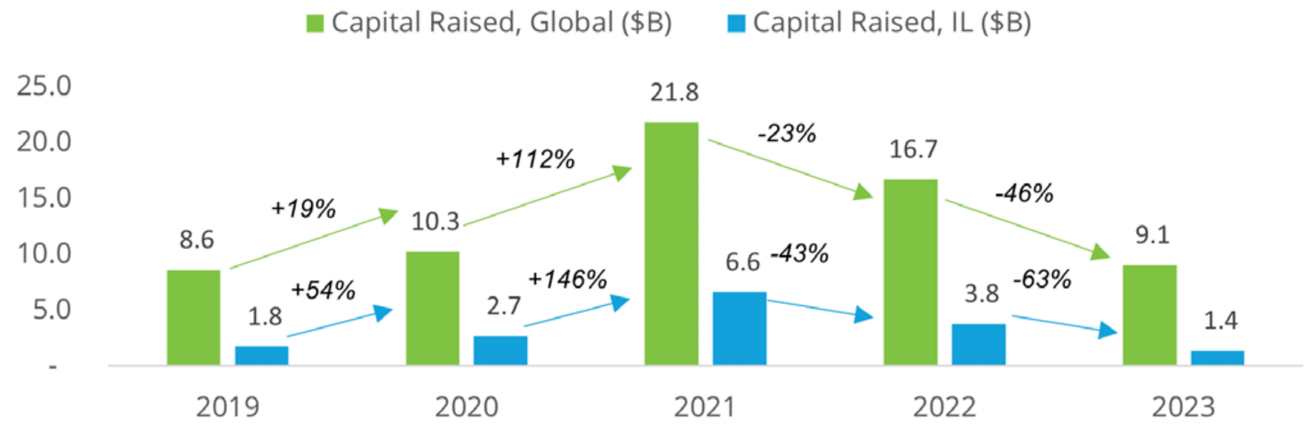


Source: "Companies' Survey", Israel Innovation Authority (December 2023)

The Israeli Cyber Sector

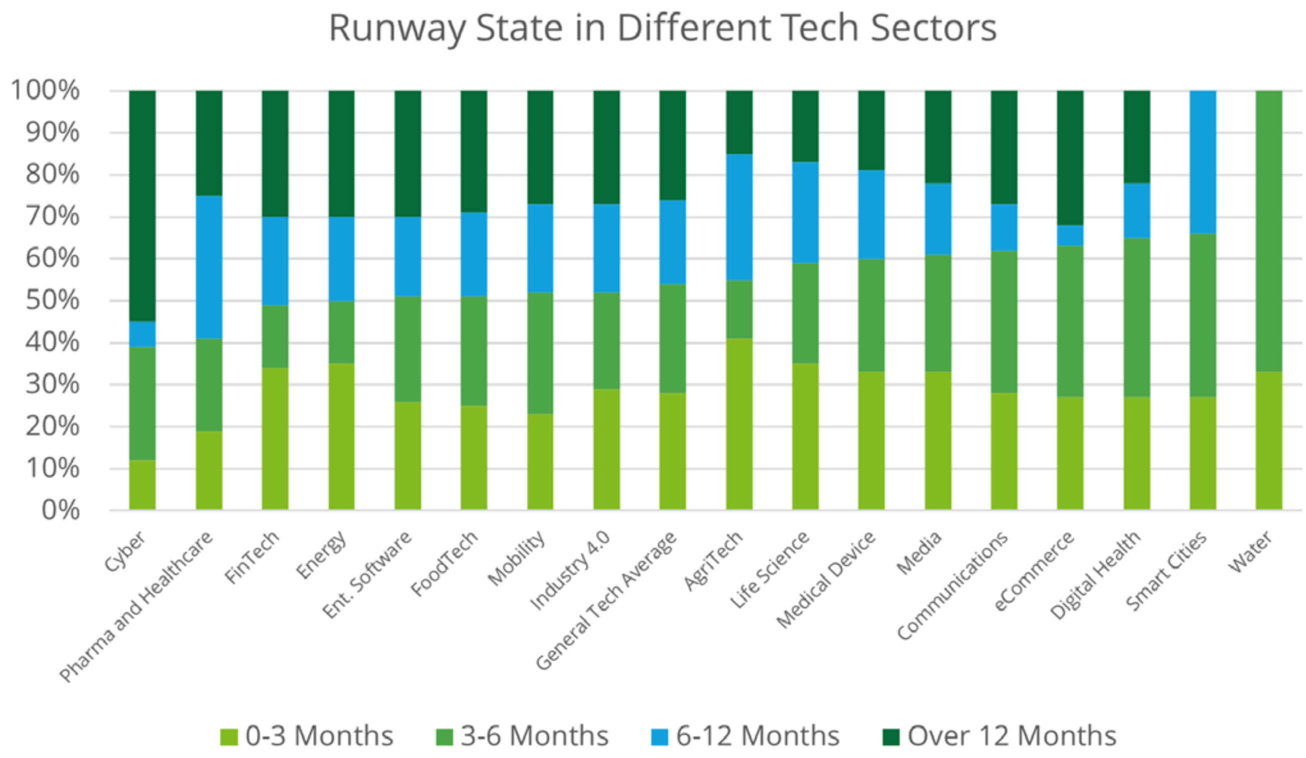
The decline in access to capital and exits within the technology industry over the past two years is mirrored in the cybersecurity sector, albeit with a more measured impact. Notably, the cyber sector stands out as the tech sector probably exhibiting a high correlation to global trends (ρ>0.9), thus indicating an anticipated recovery in 2024-2025, supported by robust consolidation and M&A activity.

Capital raised by cyber companies: Global vs. Israel (ρ>0.9)



Source: Pitchbook, as of December 31st 2023.

While the cybersecurity sector fares better than the broader tech industry, it's noteworthy that nearly 40% of companies within this sector have less than a 6-month runway, in contrast to the 56% average observed across the entire tech industry.



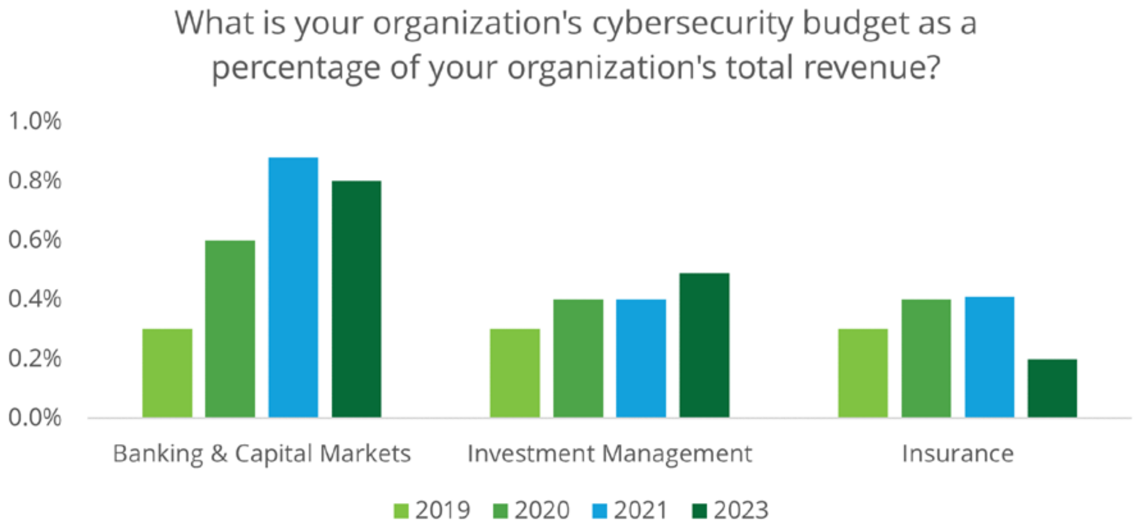
Source: "Companies' Survey", Israel Innovation Authority (December 2023)

Global Cybersecurity Budget

The ongoing digital transformation is affecting the cybersecurity industry and remains a pivotal catalyst for the widespread adoption of cybersecurity measures, in addition to increasing regulatory pressure. This trend is mirrored in the offering of certain cybersecurity companies, where a heightened emphasis on regulatory management approaches is evident.

In a recent Deloitte Survey for financial institutions, we have seen that spending relative to organizations' revenue fell slightly lower from 0.72% in 2021 to 0.54% in 2023[3]. The fact that the cyber budgets are measured as percentage of total revenues, not just as part of IT budgets, is a direct outcome of the broad impact of cyber on the entire business activities. This decline in budgets relative to revenues may also drive consolidation between cyber companies to be able to offer a centralized customer centric offering.

Source:(3) "Cybersecurity insights 2023: budgets and benchmarks for financial institutions", Deloitte (June 2023).



Source: " Cybersecurity insights 2023: budgets and benchmarks for financial institutions", Deloitte (June 2023).

Source: (5) "Final Ruling for Cybersecurity, risk management Strategy, Governance and Incident Disclosure", SEC (July 2023)

A notable shift in the cybersecurity industry in 2023, includes a stronger focus towards business impact and risk management, rather than just focusing on technology challenges. This shift marks a deeper integration of cybersecurity into organizational strategies[4].

The main two forces pushing cybersecurity spend in organizations:

- **Digital Transformation:** Emerging technologies, strongly fueled by COVID-19 digital tailwinds, require more cybersecurity protection, especially for financial services and institutions.
- **Risk Reduction:** Regulators are increasingly focused on requiring reporting on cybersecurity threats and defense posture of organizations. This is expected to increase as the SEC issued earlier this year a final ruling to adopt new regulations from all public companies[5].

We believe these forces have the potential to drive higher growth in cyber companies that support digital transformation and/or regulatory requirements in the relevant markets.

Cybersecurity M&A Scenarios

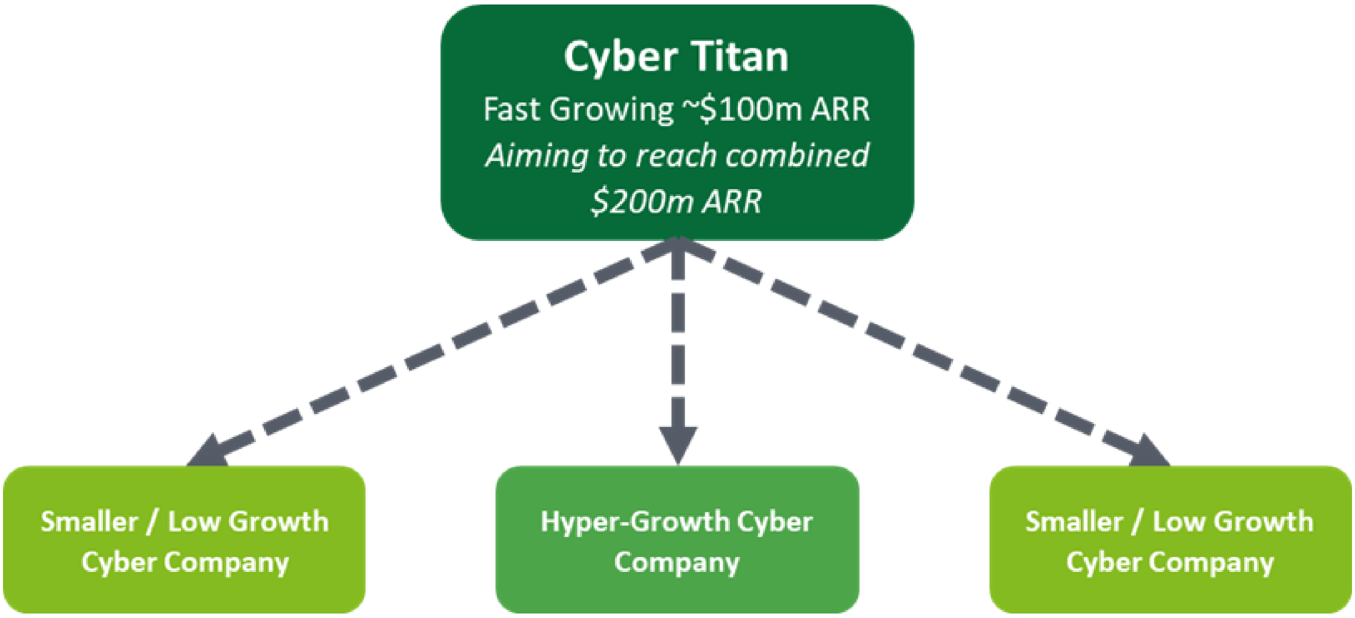
The COVID-19 period spanning 2019-2022 acted as a robust catalyst for the entire tech ecosystem, with multiples frequently experiencing significant expansion, at times reaching high double-digit, and even triple-digit figures. This surge was further propelled by investors who prioritized growth over profitability. However, since then, multiples have changed, allowing us to categorize growth cybersecurity companies into two distinct types:

- Hyper-growth companies that can sustain impressive double-digit Annual Recurring Revenue (ARR) multiples ranging from 15x to 20x and above. These multiples, or even higher, become pertinent when cybersecurity companies acquire other rapidly growing companies with complementary technologies. Consequently, buyers are willing to pay a premium to enhance the value of their offerings. Consequently, buyers are willing to pay a premium to enhance the value of their offerings.

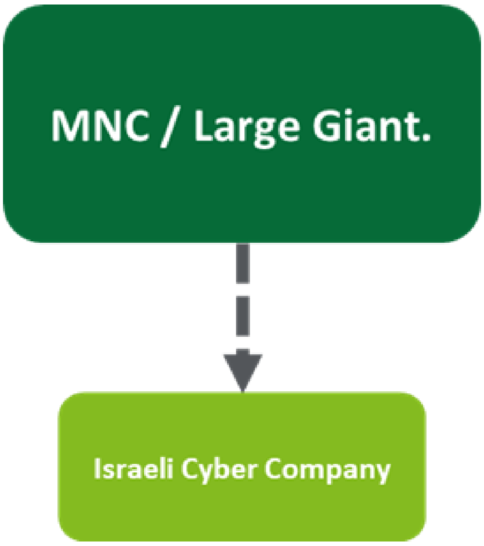
- Slow growth companies that are reluctantly being valued at 4x-6x ARR multiples. These companies might be acquisition targets for larger cyber companies or to MNCs.

Some larger companies are seeing these times as an opportunity and are doing strategic M&A processes. We believe such consolidation trend can be viewed as part of a healthy ecosystem and may continue even further into 2024-2025.
Based on our analysis, we believe that the market may experience high M&A activity in the cyber sector. Different strategic synopsis may drive such activity:

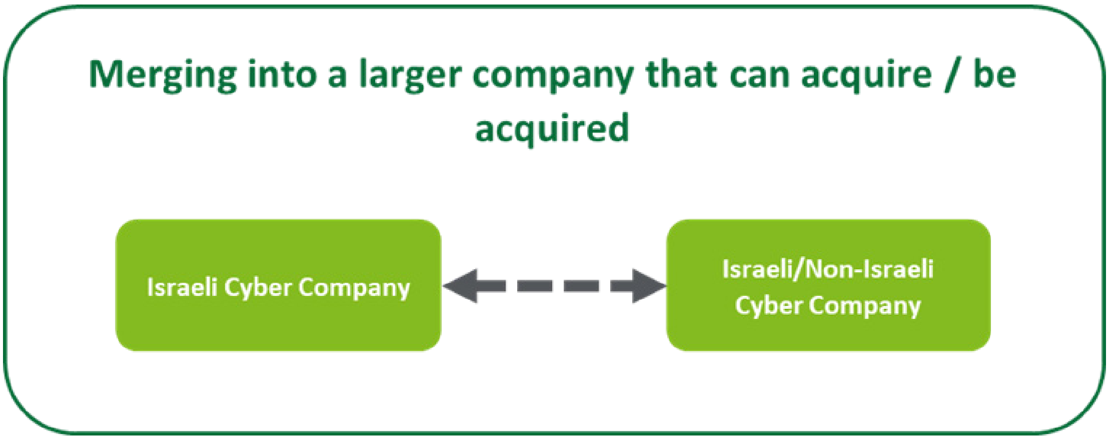
1. Scale Up through M&A for IPO Readiness - In this case, a fast-growing cyber titan with ~$100m ARR would acquire smaller cyber companies in its category or a different category in order to become a >$200m ARR company with higher readiness for an IPO.


Cyber Titan
Fast Growing ~$100m ARR
Aiming to reach combined $200m ARR
Smaller / Low Growth Cyber Company
Hyper-Growth Cyber Company
Smaller / Low Growth Cyber Company

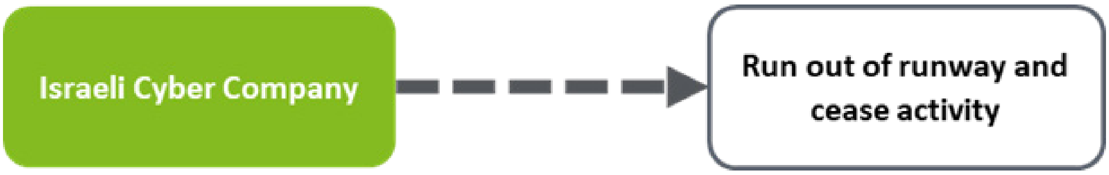
2. Traditional M&A – A large multinational corporation or tech giant acquiring a local Israeli cyber company



3. Joining Forces to become a Titan – Consolidation activities, where two or more small to medium-sized players come together through mergers to form a larger entity with a substantial market presence. The resulting merged company would possess the scale necessary to align with one of the scenarios.


Merging into a larger company that can acquire / be acquired
Israeli Cyber Company
Israeli/Non-Israeli Cyber Company

4. The inevitable ending for some companies – Reluctantly, some companies will not be able to raise before running out of cash and eventually cease activity.



These scenarios may drive the rise of global, centralized, and consolidated cybersecurity companies, offering a wider span across the organizations' offerings, geographic locations, and needs. Note that more than 75% of CISOs said they are pursuing vendor consolidation in their cybersecurity strategy [(6)]. This consolidation is motivated by risk posture improvement, rather than from budget needs.

Source: (6) "Cybersecurity insights 2023: budgets and benchmarks for financial institutions", Deloitte (June 2023).

Appendix A:

Cybersecurity Categories' Analysis

We have compiled data on nearly 300 private Israeli or Israeli-affiliated cybersecurity companies (with Israeli founders).

This encompasses exclusively active private entities, excluding both publicly traded companies and those that have undergone acquisition.

Table 1.1: Top Cyber Sectors by Number of Active Companies [7]

Category	Number of Companies
Vulnerability & Risk Management	39
IoT	33
Data Security & Privacy	28
Application Security	24
Security Operations	24

The cybersecurity sector employs over 23,500 individuals, with a majority in Israel. The top 10 companies collectively account for more than 7,500 employees.

Table 1.2: Cyber sectors with highest number of employees [7]

Category	Total Employees
Application Security	3,068
Vulnerability & Risk Management	2,965
Cloud Security	2,648
Endpoint Security	2,326
IoT	1,829

Vulnerability and Risk Management attract the highest amount of capital, as being the main perception of cybersecurity's role including SOC and threat intelligence. Often this category also spans across other categories and covers threats originating from different interfaces.

Table 1.3: Cyber sectors and capital raised [7]

Category	Total Raised ($M)
Vulnerability & Risk Management	2,606
Application Security	2,317
Cloud Security	2,107
Network Security	1,410
Endpoint Security	1,335

Source: IVC, as of December 31, 2023

Key Facts and Figures of the Cyber Categories

2.1. Vulnerability & Risk Management

The systematic process of identifying, evaluating, and prioritizing vulnerabilities and risks in an organization's IT infrastructure, and implementing appropriate controls and mitigation strategies to reduce the likelihood and impact of security incidents.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
39	2,965	2,606

Significant Companies by Capital Raised:

1. Pentera Security Ltd
2. Axonius, Inc.
3. Coro Cyber Security Ltd

2.2. IoT

The practice of securing interconnected devices and systems on the Internet of Things (IoT) ecosystem, including the protection of device hardware, software, data, and communication protocols from unauthorized access and manipulation.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
33	1,829	1,273

Significant Companies by Capital Raised:

1. Claroty Ltd
2. Upstream Security Ltd
3. Cylus Ltd

2.3. Data Security & Privacy

The implementation of technical, administrative, and physical controls to protect the confidentiality, integrity, and availability of sensitive data, and to ensure compliance with data protection regulations and industry standards.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
28	2,283	1,271

Significant Companies by Capital Raised:

1. OwnBackup Inc
2. BigID, Inc
3. Cyera US Inc

2.4. Security Operations

This sector of cybersecurity involves the ongoing, day-to-day processes, technologies, and practices aimed at detecting, analyzing, responding to, and mitigating security incidents and threats within an organization's IT environment.

Security Operations, often abbreviated as SecOps, is the proactive management and monitoring of an organization's security infrastructure, including the use of security information and event management (SIEM) systems, threat intelligence, and incident response procedures to detect, analyze, and respond to security incidents in real-time.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
24	1,149	583

Significant Companies by Capital Raised:

1. Cyber Hunters Ltd
2. Cyesec Ltd
3. Cyberbit Ltd

2.5. Web Security

The protection of web-based assets, including web applications, websites, and web services, from attacks and unauthorized access through the use of firewalls, intrusion detection and prevention systems, and web application security testing.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
16	628	302

Significant Companies by Capital Raised:

1. Namogoo Technologies Inc.
2. Source Defense Ltd
3. Guardio Ltd

2.6. Application Security

The practice of securing software applications throughout their lifecycle, including the identification and remediation of vulnerabilities in the design, development, testing, deployment, and maintenance stages, and the implementation of secure coding practices and security controls.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
24	3,086	2,317

Significant Companies by Capital Raised:

1. Snyk Limited
2. Salt Security Inc
3. NoName Gate Ltdd

2.7. Identity & Access Management

The management of digital identities and the enforcement of access controls to ensure that only authorized users have access to sensitive resources and information within an organization.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
19	1,193	1,068

Significant Companies by Capital Raised:

1. Transmit Security, Inc
2. Semperis Technologies, Inc
3. SilverFort, Inc.

2.8. Fraud & Transactions

The use of advanced analytics, machine learning, and behavioral biometrics to prevent, detect, and mitigate fraudulent activities in financial transactions, and to ensure the security and integrity of payment systems.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
17	1,809	843

Significant Companies by Capital Raised:
1. BioCatch Ltd
2. Cheq AI Technologies Ltd
3. ActiveFence Ltd

2.9. Endpoint Security

The protection of endpoint devices, such as laptops, desktops, smartphones, and tablets, from threats and unauthorized access through the use of antivirus, anti-malware, and personal firewall software, and the implementation of security policies and controls.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
16	2,326	1,335

Significant Companies by Capital Raised:
1. CyberReason Inc
2. Deep Instinct Inc
3. Cynet Security Ltd

2.10. Network Security

The protection of an organization's network infrastructure and the data transmitted over it from unauthorized access, misuse, and disruption through the use of firewalls, intrusion detection and prevention systems, virtual private networks (VPNs), and other security technologies.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
23	1,630	1,410

Significant Companies by Capital Raised:
1. Cato Networks Ltd
2. Island Technology, Inc
3. Cyolo Ltd

2.11. Cloud Security

The implementation of security controls and best practices to protect data, applications, and infrastructure in cloud computing environments, and to ensure compliance with industry standards and regulations.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
14	2,648	2,107

Significant Companies by Capital Raised:

1. Wiz, Inc
2. Orca Security Ltd
3. Aqua Security Software Ltd

2.12. Threat intelligence

The collection, analysis, and dissemination of actionable information about current and emerging threats to an organization's security, including indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs) used by threat actors, and recommended mitigation strategies.

Threat intelligence is the structured and analyzed information about potential or existing cyber threats, including their context, mechanisms, indicators, and implications. It encompasses data collected from various sources, such as security feeds, open-source intelligence, forums, dark web monitoring, and incident reports, that is then processed, contextualized, and used to understand, anticipate, and mitigate cyber threats.

Threat intelligence aims to provide actionable insights into emerging threats, attack patterns, vulnerabilities, and malicious activities, enabling organizations to make informed decisions, strengthen their security posture, and proactively defend against cyber threats. It involves the collection, analysis, and dissemination of intelligence to support security operations, incident response, and overall cybersecurity strategies.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
11	545	272

Significant Companies by Capital Raised:

1. Cybertoka Ltd
2. CyberInt Technologies Ltd
3. Kela Research and Strategy Ltd

2.13. SaaS Security

The practice of securing data and applications in Software as a Service (SaaS) environments, including the implementation of access controls, data encryption, and security monitoring, and the evaluation of SaaS providers' security practices and compliance with industry standards.

SaaS security ensures that organizations using cloud-based software services can mitigate risks associated with data breaches, unauthorized access, data loss, and service disruptions, thereby maintaining the security and reliability of their SaaS applications and the data stored within them.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
9	379	237

Significant Companies by Capital Raised:
1. A.S. Adaptive Shield Ltd
2. Docontrol, Inc
3. Astrix Security Ltd

2.14. Blockchain Security

The protection of blockchain-based systems and applications from threats and unauthorized access, including the securing of smart contracts, consensus mechanisms, and cryptographic protocols, and the mitigation of risks associated with blockchain technology.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
8	777	1,210

Significant Companies by Capital Raised:
1. Fireblocks Inc
2. Certora Ltd
3. dWallet Labs Ltd.

2.15. Email Security

The protection of email systems and accounts from spam, phishing, and other email-based threats using email filtering, encryption, and authentication technologies, and the implementation of security awareness training and best practices.

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
5	344	209

Significant Companies by Capital Raised:

1. Ironscales Ltd
2. Perception Point Ltd
3. Re-Sec Technologies Ltd

2.16. Mobile Security

Key Facts and Figures:

Number of Companies	Total Employees	Total Raised ($M)
5	291	70

Significant Companies by Capital Raised:

1. Appdome Inc
2. Communitake Technologies Ltd
3. Safehouse Technologies Ltd

He protection of mobile devices and the data stored on them from threats and unauthorized access through the use of mobile device management (MDM) and mobile application management (MAM) solutions, and the implementation of security policies and controls.

Endnotes

1. “Iron Swords, Point of View”, Deloitte Monitor Israel (December 2023)
2. “Companies’ Survey”, Israel Innovation Authority (December 2023)
3. “Cybersecurity insights 2023: budgets and benchmarks for financial institutions”, Deloitte (June 2023)
4. “Cybersecurity insights 2023: budgets and benchmarks for financial institutions”, Deloitte (June 2023)
5. “Final Ruling for Cybersecurity, risk management Strategy, Governance and Incident Disclosure”, SEC (July 2023)
6. “Cybersecurity insights 2023: budgets and benchmarks for financial institutions”, Deloitte (June 2023).

Contact us

Tal Chen
Partner
Corporate Finance Advisory
Deloitte Israel
talchen@deloitte.co.il

Eyal Schwartz
Managing Director
Corporate Finance Advisory
Deloitte israel
elschwartz@deloitte.co.il

Lior Kalev
Partner,
Head of IL Cyber Center
Deloitte Israel
lkalev@deloitte.co.il

Disclaimer

This Report was carried out by Deloitte Israel &Co ("Deloitte"). This Report is based on public information. The data, information, explanations and representations that we have used for the purpose of preparing the Report, has not been independently verified by us, and we do not express an opinion as to their completeness, correctness or accuracy, but only its reasonableness and under no circumstances shall we be liable for any loss, damage, cost or expense incurred in any way through fraud, misrepresentation, deception, provision of Information that is incorrect and incomplete or withholding information.

Any use, which any party, makes of this Report or any reliance on, or decisions to be made based on it, is the responsibility of that party. By using this Report, such party consents that Deloitte has no liability with respect to such reliance or decisions. Deloitte accepts no liability for damages, if any, suffered by any party as a result of decisions made or actions taken based on this Report.

For the avoidance of doubt: (a) No party who receives Report or will be exposed to the Report will be considered a Deloitte client; (b) No duty of care or liability on Deloitte's part with respect to a party that is exposed to the Report shall be created and it shall not be deemed as if any business relationship has been established between Deloitte and that party; (c) Deloitte shall not be liable for any use by any party of the Report.

The information presented in this report reflects public information as presented on databases and may differ from proprietary data related to private companies.

Deloitte.

www.deloitte.co.il