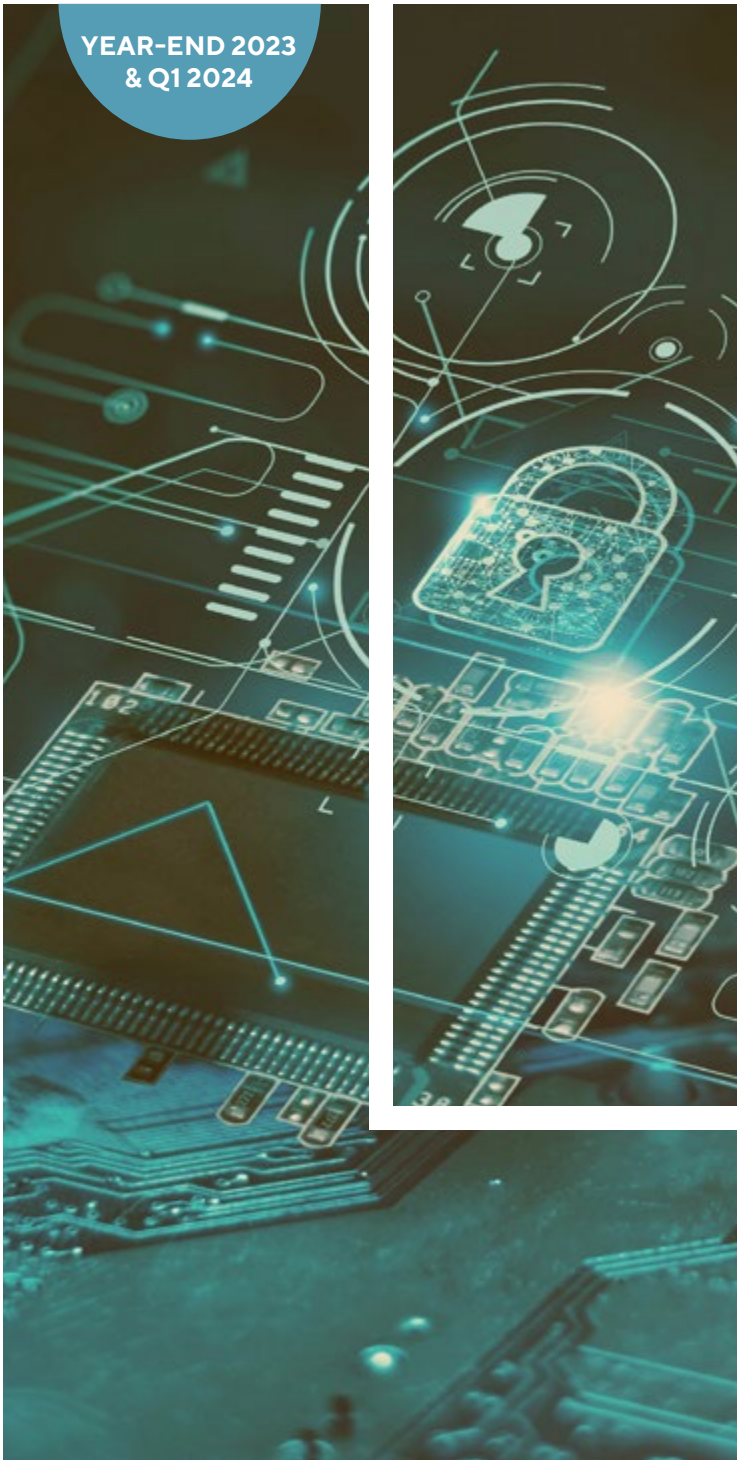
SECURITY & INFRASTRUCTURE SOFTWARE

Cybersecurity Report



INSIDE THIS ISSUE

- In 2023, cybersecurity M&A activity saw a significant decline in both volume and value, reaching its lowest point since 2014, attributed to factors such as high interest rates, inflation and geopolitical tensions
- However, Q1 M&A activity indicated a strong start to the year, with transaction numbers seeing a sharp increase over Q4 2023, potentially signaling that the M&A market is poised for a strong recovery throughout the year
- Despite market challenges, cyber venture / growth investing in 2023 remained in-line with historical averages, signaling high availability of growth capital for cyber innovation; furthermore, stable or declining interest rates in 2024 are expected to boost growth investment activity, particularly in cybersecurity, which has strong secular demand trends and an above-average growth outlook
- In 2024, cybersecurity trends include the integration of AI for enhanced threat detection, increased focus on cloud security due to growing reliance on cloud services, the necessity for navigating complex regulatory compliance requirements, adoption of Zero Trust architectures for evolving threat landscapes, elevation of cybersecurity as a board-level concern, emphasis on building cyber resilience through preparation and recovery strategies and increased focus on IoT and IIoT with rising geopolitical tensions increasing compliance and security needs for cyber physical systems

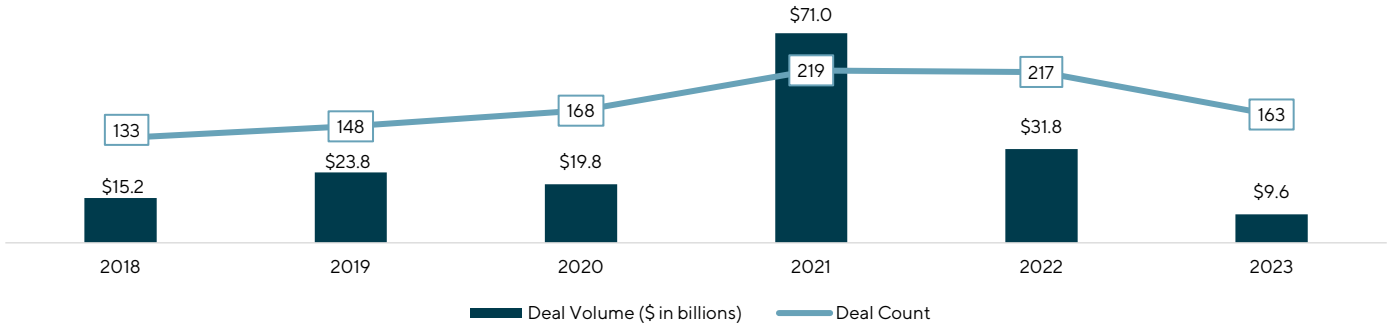
LINCOLN INTERNATIONAL

2023 and Q1 2024 Cybersecurity M&A Activity

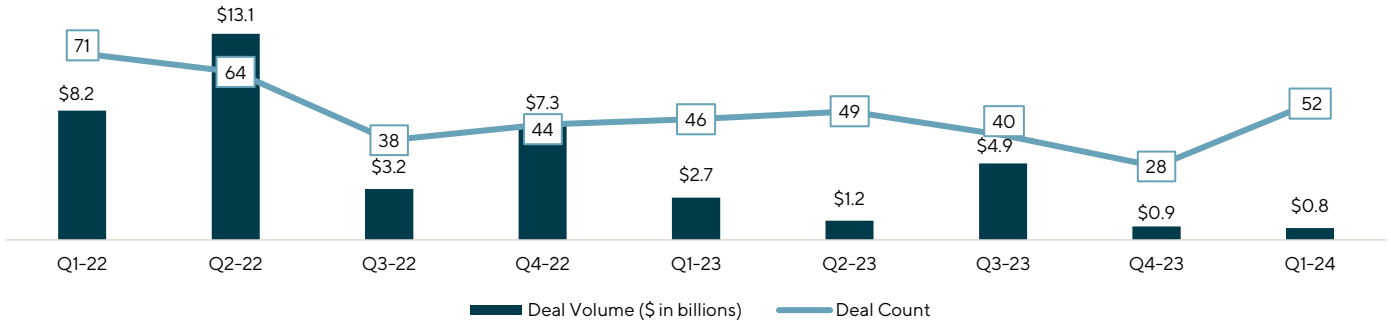
OVERVIEW

- Cybersecurity M&A activity levels and values experienced a significant decline in 2023, as high interest rates, inflation and geopolitical tensions continued to weigh on the global economy
- Global cybersecurity M&A deal volume reached $9.6 billion in 2023, well below the record highs seen in 2021 and 2022, and represents the lowest annual volume since 2014
- Acquisition deal count in 2023 remained more resilient at 163 transactions, 25% below 2022's 217 and 26% below 2021's 219 deals. However, 2023's transaction count remained strong compared to historical averages, surpassing the 10-year average by 6%
- While most sector M&A transactions do not have publicly disclosed multiples, available data shows an overall median sector enterprise value / LTM revenue multiple of 6.0x in 2023, versus 8.9x in 2022 and 7.4x in 2021
- While Q3 2023 saw a sharp uptick in cybersecurity M&A deal volume, Q4 closed out the year posting the lowest quarterly deal volume since Q2 2017. On a positive note, the lack of volume in 2023 has created a substantial backlog of assets that, in combination with improving economic conditions, will likely fuel a more active deal market in 2024
- Q1 2024 M&A activity indicates a strong start to the year, with consecutive quarterly activity rising sharply in Q1 2024 to 52 transactions, up from 28 in Q4 2023. Deal volume remained largely flat at $759 million compared to $859 million in Q4
- Year-over-year quarterly sector M&A volume remained flat in Q1 2024 with 52 cybersecurity transactions, compared to 46 in Q1 2023. However, year-over-year Q1 deal volume fell significantly to $759 million in the quarter vs. $2.7 billion the year before
- With public markets beginning to stabilize and the perceived lower risk of increasing interest rates, we see financial sponsors continuing to play a significant role in M&A, driven by the need for pre-IPO unicorns to scale and enhance their capabilities
- Enterprises are increasingly streamlining their cybersecurity portfolios, spurred by CISOs' "tool fatigue" and the push for unified security frameworks. This shift is expected to drive M&A activities as firms aim to provide all-encompassing, integrated security offerings tailored to evolving customer requirements

ANNUAL CYBER M&A ACTIVITY

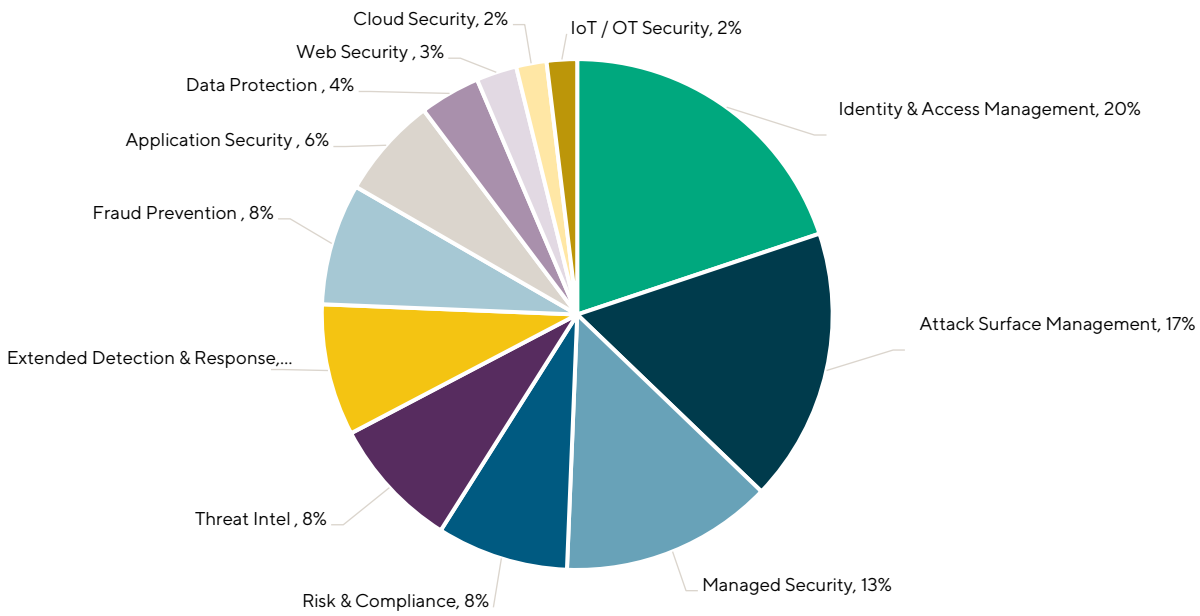


QUARTERLY CYBER M&A ACTIVITY



Sources: 451 Research / S&P Capital IQ, Crunchbase, PitchBook, public sources and Lincoln estimates

2023 CYBER M&A TRANSACTIONS BY VERTICAL



NOTABLE 2023 AND Q1 2024 CYBERSECURITY M&A TRANSACTIONS

Announced	Acquirer	Target, Subsector	Deal Value / Multiple of LTM Revenues	Announced	Acquirer	Target, Subsector	Deal Value / Multiple of LTM Revenues
Mar-24	zscaler	Avalor Data Security	$350 million / ND	Aug-23	rubrik	Laminar Data Security	$220 million / 32.0x
Feb-24	HAVELI	ZEROFOX Attack Surface Management	$350 million / 1.6x	Jul-23	THALES	imperva Data & App Security	$3.6 billion / 6.1x
Jan-24	Hewlett Packard Enterprise	JUNIPER NETWORKS Network Security	$12.8 billion / 2.3x	Jul-23	CISCO	ORT Identity & Access Management	ND / ND
Nov-23	paloalto NETWORKS	TALON Endpoint Security	$625 million / ND	Jul-23	SpireCapital	COBWEBS TECHNOLOGIES Threat Intelligence	$200 million / 5.0x
Oct-23	ARCTIC WOLF	revelstoke SOAR	ND / ND	Jun-23	THALES	tesserent Security Consulting & Services	$120 million / 1.2x
Oct-23	proofpoint	TESSIAN Email Security	$300 million / 7.5x	May-23	CROSSPOINT CAPITAL	ABSOLUTE Endpoint Security	$870 million / 3.9x
Oct-23	Rockwell Automation	VERVE Endpoint Security	$185 million / 5.8x	Mar-23	hp	axis Zero Trust Network Access	$500 million / ND
Sep-23	paloalto NETWORKS	Dig Data Security	$350 million / ND	Mar-23	SUMMAEQUITY	LOGPOINT SIEM / SOAR	$150 million / 6.0x
Sep-23	tenable	ermetic Cloud Infrastructure Security	$265 million / 26.5x	Feb-23	CISCO	VALTIX Cloud Security	$125 million / 25.0x
Aug-23	CHECK POINT	perimeter 81 Zero Trust Network Access	$490 million / 24.5x	Feb-23	FP FRANCISCO PARTNERS	sumo logic SIEM / SOAR	$1.7 billion / 4.8x

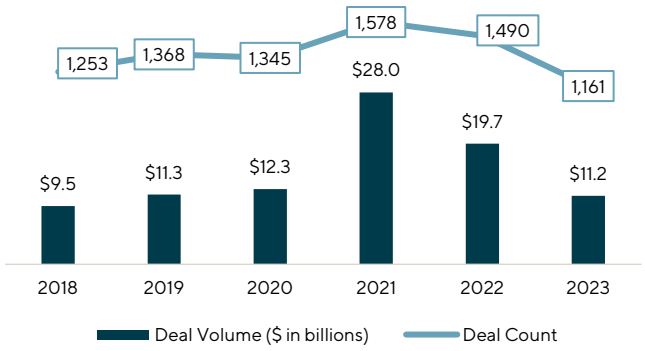
Sources: 451 Research / S&P Capital IQ, Crunchbase, PitchBook, public sources and Lincoln estimates

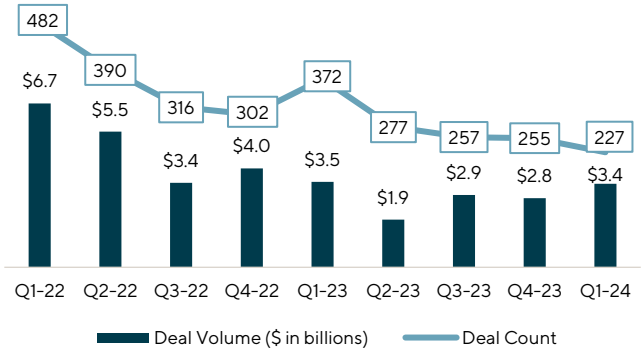
2023 and Q1 2024 Cybersecurity Investment Activity

CYBER GROWTH INVESTING SHOWED RESILIENCE IN A TURBULENT MACRO ENVIRONMENT

- Despite market headwinds, 2023 cyber venture / growth investing remained resilient, finishing the year with total funding of $11.2 billion across 1,161 companies, in line with historical averages and signaling that available growth capital for cyber innovation remains high
- Despite an improving economic climate, Q1 2024 investing activity declined on a year-over-year and consecutive quarter basis, signaling some lingering uncertainty
- However, the outlook for 2024 remains positive overall, as stable or declining interest rates are poised to fuel an uptick in growth investment activity across various sectors. With the cybersecurity sector boasting strong secular demand trends and an above-average growth outlook, there are compelling reasons to be optimistic about the investment landscape in 2024

ANNUAL & QUARTERLY CYBER GROWTH ACTIVITY





NOTABLE 2023 AND Q1 2024 CYBERSECURITY GROWTH INVESTMENTS

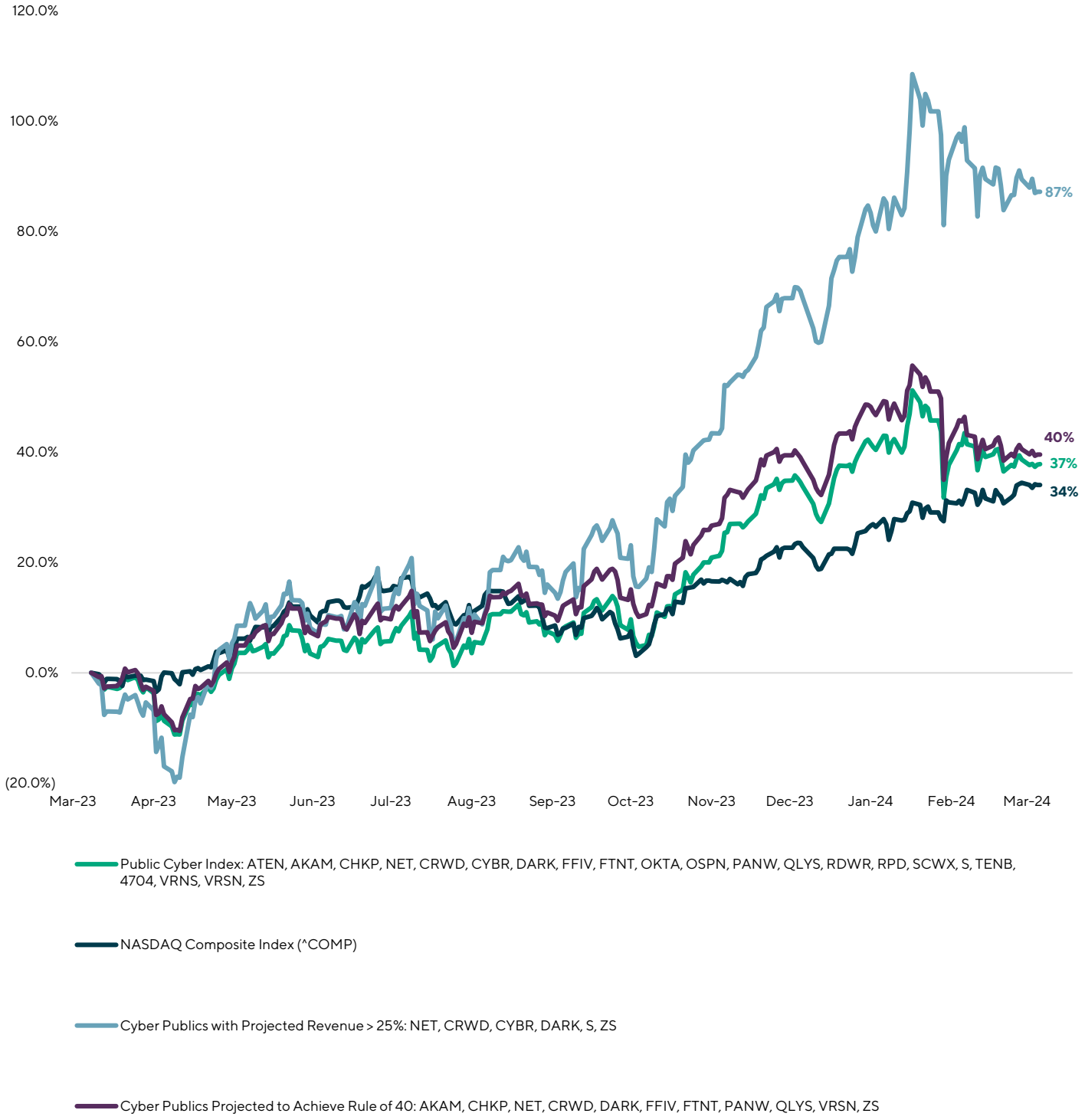
Announced	Company	Subsector	$ Raised in Round	Announced	Company	Subsector	$ Raised in Round
Mar-24	AXONIUS	IoT Security	$200 million	Jul-23	netcraft	Digital Risk Management	$100 million
Mar-24	CLAROTY	Cyber-Physical Systems Protection	$100 million	Jun-23	CYERA	Data Security	$100 million
Jan-24	ExtraHop	Network Security	$100 million	Jun-23	blackpoint	Managed Detection & Response	$190 million
Jan-24	aqua	Cloud Security	$195 million	Apr-23	CORO	Cloud Security	$75 million
Nov-23	BlueVoyant	Managed Security Services	$140 million	Apr-23	ID.me	Identity & Access Management	$132 million
Aug-23	SpyCloud	Threat Intelligence	$110 million	Apr-23	cybereason	Endpoint Security	$100 million
Aug-23	CATO NETWORKS	Secure Access Service Edge	$238 million	Feb-23	WIZ	Cloud Security	$300 million
Aug-23	resilience	Risk & Compliance	$100 million	Feb-23	deepwatch	Managed Security Services	$180 million

Sources: 451 Research / S&P Capital IQ, Crunchbase, PitchBook, public sources and Lincoln estimates

Cybersecurity Public Index Materially Outperforms NASDAQ

PUBLIC CYBER VALUATIONS HAVE EXHIBITED A MASSIVE RECOVERY SINCE EARLY-2023 LOWS

- Over the last 12 months, the Index of Public Cyber Vendors increased by 37%, outpacing the NASDAQ which increased by only 34% over the same period
- Through the end of Q1, the Index of Public Cyber Vendors has surged by 66% from its three-year low recorded on January 5, 2023, showcasing the continued strength of the sector alongside a broader recovery of public valuations
- Through early 2024, markets have rewarded the most aggressive growers, with cyber publics expected to achieve greater than 25% revenue growth in 2024 seeing their stock prices increase by 87% over the last twelve months. Conversely, cyber publics expecting to achieve a balanced growth and profitability profile (Rule of 40) in 2024 have seen their valuations rise by just 40% over the same period



Revenue Growth is Once Again the Most Critical Driver for Cyber Valuations

REVENUE GROWTH HAS DISPLACED RULE OF 40 AS THE PRIMARY VALUATION INDICATOR

- Starting in 2H 2022, balanced growth and profitability (Rule of 40) became the primary driver of public valuations, displacing revenue growth. This shift was driven by rising interest rates and somewhat tightening access to capital
- However, with the market recovery in early 2024, this trend has reversed, with the most aggressive growers being rewarded the most in the public markets, regardless of profitability levels
- As of the time of this writing, revenue growth had a 65% correlation with public cyber vendor 2024E enterprise value / revenue multiples. In comparison, Rule of 40 had just a 62% correlation with 2024E revenue multiples

CYBER PUBLIC PERFORMANCE

	2024E Revenue Growth	2024E EBITDA Margin	Rule of 40[1]	Actual vs. Estimated Results[2]		EV / Revenue 2024E[3]
				Reveue ($ in millions)	EPS	
Cloudflare	27.90%	19.30%	47.20%	Beat by $5.2, 1.4%	Beat by $0.03, 22.6%	15.3x
CrowdStrike	26.30%	27.70%	54.00%	Beat by $5.4, 0.6%	Beat by $0.06, 6.6%	14.9x
VeriSign	7.00%	73.20%	80.30%	Beat by $2.5, 0.6%	Beat by $0.05, 2.7%	11.9x
Zscaler	25.40%	22.90%	48.30%	Beat by $18.2, 3.6%	Beat by $0.11, 17.4%	10.4x
Palo Alto Networks	14.50%	29.20%	43.70%	Beat by $3.5, 0.2%	Beat by $0.21, 16.9%	9.8x
CyberArk Software	22.30%	16.60%	38.90%	Beat by $8.3, 3.9%	Beat by $0.48, 173.2%	9.5x
Qualys	10.30%	42.00%	52.30%	Met Expectations	Beat by $0.14, 11.1%	8.6x
Varonis Systems	12.80%	8.10%	20.90%	Beat by $0.3, 0.2%	Beat by $0.06, 67.2%	7.9x
Fortinet	13.90%	29.80%	43.70%	Beat by $13.5, 1.0%	Beat by $0.05, 11.8%	7.7x
Check Point Software	5.40%	44.90%	50.30%	Beat by $3.9, 0.7%	Beat by $0.03, 1.7%	6.6x
SentinelOne	28.50%	7.60%	36.10%	Beat by $4.8, 2.8%	Beat by $0.03, 56.9%	6.0x
Okta	13.10%	19.80%	32.90%	Beat by $17.4, 3.0%	Beat by $0.08, 15.5%	5.8x
Tenable	13.90%	20.30%	34.30%	Beat by $2.5, 1.2%	Beat by $0.08, 43.4%	5.6x
Akamai Technologies	7.60%	43.10%	50.70%	Miss by -$2.2, -0.2%	Beat by $0.03, 2.0%	4.4x
Darktrace	21.00%	22.10%	43.10%	N/A	N/A	3.9x
Rapid7	11.80%	21.30%	33.10%	Beat by $1.1, 0.5%	Beat by $0.01, 2.2%	3.8x
F5	4.30%	39.00%	43.30%	Miss by -$2.9, -0.4%	Beat by $0.04, 1.5%	3.6x
A10 Networks	8.40%	29.70%	38.20%	Beat by $1.2, 2.1%	Beat by $0.02, 9.7%	3.0x
Trend Micro	6.60%	28.80%	35.40%	Beat by $12.6, 3.0%	N/A	2.6x
Radware	6.60%	10.10%	16.70%	Beat by $1.5, 2.4%	Beat by $0.02, 14.5%	1.7x
OneSpan	3.50%	23.50%	27.00%	Beat by $8.4, 15.0%	Beat by $0.26, 156.7%	1.6x
SecureWorks	4.50%	4.70%	9.30%	Beat by $2.0, 2.3%	Beat by $0.09, 1299.4%	1.5x

Note: (1) Calculated as 2024 projected revenue growth plus 2024 projected EBITDA margin; (2) As of latest quarter reported; (3) Multiples as of 03/31/2024

Looking Ahead to 2024 and Beyond

AI Expansion
The integration of artificial intelligence (AI) into cybersecurity is transforming the landscape of digital security. These technologies are enhancing the capabilities of cybersecurity solutions by improving threat detection and automated response mechanisms. However, as these technologies advance, they also present new challenges and opportunities for both defenders and adversaries in the cybersecurity domain.

Cloud Security Escalation
The shift towards cloud computing has been a significant trend in the business world, driven by the need for more flexible, scalable and cost-effective IT solutions. As businesses increasingly rely on cloud services, the importance of cloud security has come into sharp focus.

Regulatory and Compliance Dynamics
As global cybersecurity regulations tighten in response to evolving threats and technologies, organizations must navigate complex compliance requirements. Adopting frameworks like the NIST Cybersecurity Framework has become essential for meeting industry-specific regulations and leveraging compliance for competitive advantage. The rise in compliance costs spurs investment in cybersecurity solutions, while continuous monitoring and incident response become critical for adhering to standards demanded by cyber insurers and regulations like GDPR and CCPA, reinforcing the need for robust data protection policies.

Zero Trust Implementation
The implementation of zero trust architectures represents a paradigm shift in cybersecurity strategy, increasingly adopted to mitigate risks within an evolving digital landscape. This security framework, guided by the principle of "never trust, always verify" is not a static solution but an ongoing process that demands continuous adaptation to the ever-changing threat environment.

Cybersecurity as a Board-Level Concern
Cybersecurity is becoming a crucial boardroom issue, fueled by the understanding that cyber risks affect overall business. Regulatory and investor pressures are making boards integrate cyber risk into their strategies. By 2026, most will likely have a cybersecurity expert, highlighting the shift towards cyber-informed governance. The emphasis is moving from just protecting assets to building cyber resilience, aligning it with the broader risk framework and developing a workforce knowledgeable in supporting this strategic transition.

Enhanced Cyber Resilience
Organizations are enhancing their cyber resilience by preparing for breaches, focusing on both prevention and quick recovery to keep business running smoothly. This approach combines advanced technology, skilled staff and effective processes, aiming to reduce operational disruptions. Motivated by strategic goals, regulatory demands and growing investments in resilience, firms are prioritizing solid backup systems, clear response plans and constant threat surveillance.

IoT and IIoT Focus
Rising geopolitical tensions, increasing prevalence and complexity of cyber attacks and accelerating regulatory oversight are creating a need for organizations to protect their cyber and physical assets, thus increasing focus and demand for cybersecurity solutions.

AREAS OF HIGH INTEREST, BROADLY DEFINED, AND ACTIVITY IN 2024 WILL LARGELY FALL INTO THESE AREAS:

- **Preparedness:** Security awareness training (non-professionals), training and certification (professionals), third-party risk / vendor risk management
- **Prevention:** API security, attack surface management, cloud application security, data privacy and encryption, threat intelligence, validation & advanced authentication, zero trust network access
- **Protection:** Cloud infrastructure protection, cloud / network security policy management, extended detection and response / SOAR, managed detection and response, SaaS app protection, secure access service edge

Recent Cyber Take-Private Activity and Leading Cyber IPO Candidates

Take-Private Announced	Acquirer	Target, Subsector	Enterprise Value	Upcoming IPO Candidate, Subsector	Most Recent Pre-Money Valuation with Equity Raise / Date[1]	Money Raised to Date[2]
Apr-24	THOMABRAVO	DARKTRACE Network Security	$5.4 billion	netskope Cloud Security	$7.2 billion / Jan-23	$1.5 billion
Feb-24	HAVELI	ZEROFOX Attack Surface Mgmt.	$350 million	ARCTIC WOLF Managed Security	$4.2 billion / Nov-23	$1.1 billion
Jan-24	Hewlett Packard Enterprise	JUNIPER NETWORKS Network Security	$14.0 billion	snyk Application Security	$7.2 billion / Jan-23	$1.1 billion
Sep-23	cisco	splunk> Data Analytics	$28.0 billion	onetrust Risk & Compliance	$4.4 billion / Jul-23	$1.1 billion
May-23	CROSSPOINT CAPITAL	ABSOLUTE Network Security	$870 million	Fireblocks Blockchain Security	$7.5 billion / May-23	$1.0 billion
Apr-23	THOMABRAVO	MAGNET FORENSICS Data Management	$1.3 billion	TANIUM Endpoint Security	$8.9 billion / May-22	$980 million
Feb-23	FP FRANCISCO PARTNERS	sumo logic Security Analytics	$1.7 billion	1Password IAM	$6.2 billion / Jan-22	$950 million
Oct-22	THOMABRAVO	ForgeRock IAM	$2.3 billion	WIZ Cloud Security	$10.0 billion / Feb-23	$800 million
Sep-22	VISTA	KnowBe4 Risk & Compliance	$4.6 billion	ARMIS IoT	$3.4 billion / Mar-24	$740 million
Aug-22	THOMABRAVO	PingIdentity IAM	$2.7 billion	Socure Fraud Prevention	$4.4 billion / Nov-21	$740 million
Aug-22	opentext	MICRO FOCUS Messaging Security	$5.8 billion	transmit security IAM	$2.2 billion / Jun-21	$580 million
May-22	BROADCOM	vmware Cloud Security	$61.0 billion	illumio Cloud Security	$2.8 billion / Aug-21	$560 million
Apr-22	THOMABRAVO	SailPoint IAM	$6.9 billion	exabeam SOC & IR	$2.2 billion / Jun-21	$430 million
Apr-22	Kaseya	datto Data Security	$6.2 billion	AXONIUS Attack Surface Mgmt.	$2.4 billion / May-22	$400 million
Mar-22	Google	MANDIANT MDR	$5.4 billion	Pindrop IAM	$810 million / Dec-22	$230 million

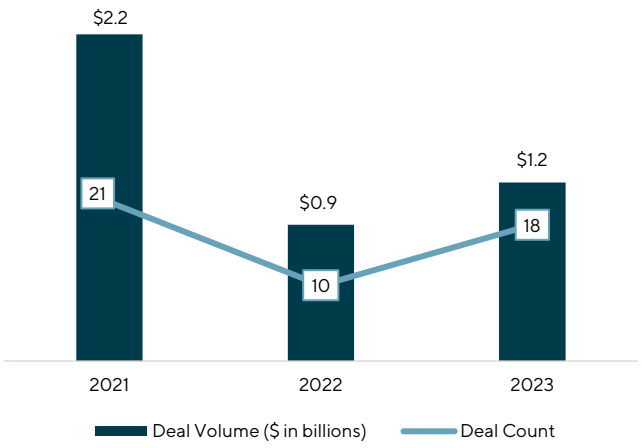
Note: (1) Includes latest disclosed series funding round; (2) Sum of known capital injected since last majority transaction or recapitalization

Cybersecurity Activity in Israel, a Capital of Cybersecurity Investment & M&A

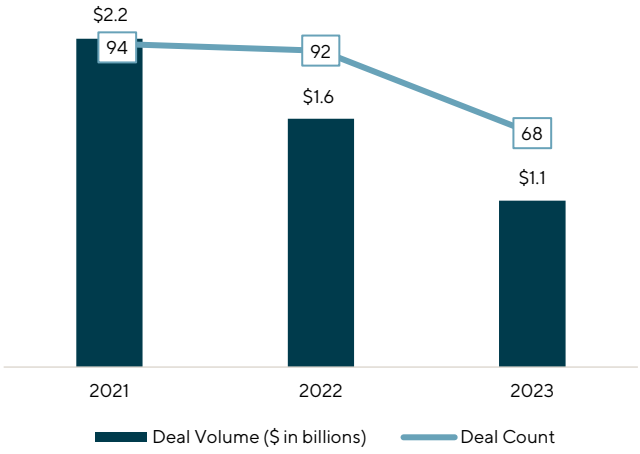
ISRAEL HAS CONTINUED TO BE AN EPICENTER FOR CYBER M&A AND GROWTH INVESTING

- Despite significant geopolitical turmoil in 2023, Israel's rapidly advancing technological and engineering expertise continues to attract investors to its market creating abundant M&A opportunities
- Despite a global M&A slump in 2023, both deal count and deal volume increased for Israel-based targets in 2023 versus 2022
- Even with decreasing investment volume and deal count in Israel-based Cyber companies year-over-year since 2021, Israel-based companies still attracted approximately 10% of the global Cyber growth investment deal volume in 2023, despite growing geopolitical tensions seen in Q3 and Q4

ISRAEL CYBERSECURITY M&A ACTIVITY



ISRAEL CYBERSECURITY GROWTH INVESTMENT ACTIVITY



RECENT ACTIVITY WITH ISRAEL-BASED CYBER COMPANIES

Announced	Acquirer	Target, Subsector	Deal Value
Mar-24	WIZ	Gem Cloud Security	$350 million
Mar-24	zscaler	Avalor Data Security	$350 million
Jan-24	Delinea	Authomize IAM	ND
Dec-23	okta	Spera IAM	$100 million
Nov-23	paloalto NETWORKS	TALON Endpoint Security	$458 million
Sep-23	paloalto NETWORKS	Dig Cloud Security	$350 million

Sources: 451 Research, PitchBook, public sources

Major Data Breaches of 2023 and 2024

DATA BREACHES HAVE HIT HIGH PROFILE TARGETS, EXPOSING SENSITIVE CLIENT INFORMATION

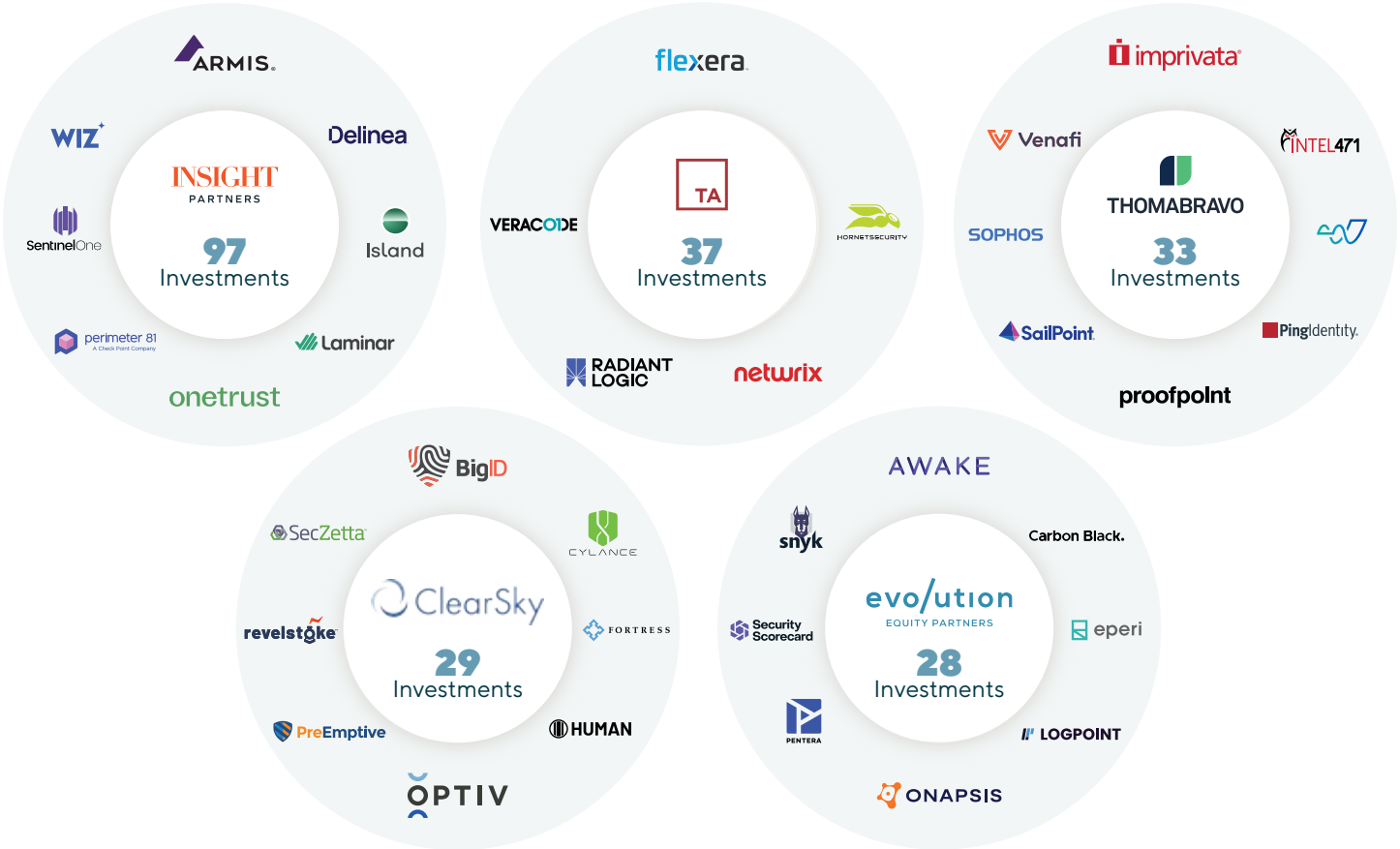
- Throughout 2023 and into 2024, hackers have consistently targeted high-profile companies for their valuable customer data, a concern that is only being accelerated with the development in the capabilities of AI
- Companies are increasingly concerned with prevention of these damaging cyber attacks and are taking preventative measures, including but not limited to hiring Chief Information Security Officers, or CISOs

RECENT MAJOR DATA BREACHES

March 2024	AT&T	AT&T revealed the social security numbers of approximately 8 million account holders and approximately 65 million former account holders were leaked by hackers to the dark web
September 2023	okta	Okta's customer support system was infiltrated, granting unauthorized access to sensitive personal information of 99.6% of Okta customers
May 2023	Progress	Progress Software's managed file transfer solution was corrupted, affecting more than 2,500 organizations and 64 million individuals

Cyber-Focused Financial Sponsor Landscape

PRIVATE EQUITY GROUPS BY TOTAL NUMBER OF CYBER INVESTMENTS (LAST 5 YEARS) AND SELECT PORTFOLIO COMPANIES



Sources: PitchBook, public sources

2024 Voice of CISO

IN TODAY'S EVER-EVOLVING SECURITY LANDSCAPE, CHIEF INFORMATION SECURITY OFFICERS PROVIDE THEIR THOUGHTS ON THE CURRENT CYBERSECURITY CLIMATE, THEIR BIGGEST CHALLENGES, TRENDS AND MORE

The Ongoing Evolution of AI Presents New Challenges to Security Protocols

- The rapid evolution of AI, specifically generative AI, poses challenges for CISOs and CIOs in crafting their 2024 plans
- AI lowers the barrier for novice cyber criminals, hackers-for-hire and hacktivists to carry out effective access and information gathering operations. This enhanced access will likely contribute to the global ransomware threat
- Adapting to changes requires a flexible strategy, complicating long-term planning as organizations aim to leverage AI's advantages while maintaining resilience

> "AI is being leveraged by bad actors to reverse engineer certain malware and decode how certain defense mechanisms in the cybersecurity space work. Cyber threat actors, both state-sponsored and independent, skilled and less skilled, are employing AI to different extents, creating a challenging environment for practitioners."
>
> *– CISO, Global Investment Bank*

On the Flip Side, AI-Driven Solutions are Poised to Deliver Significant Advancements to the Security Industry

- The adoption of AI into cybersecurity has gained strong momentum. Leading innovators are incorporating AI for early threat detection, predictive analysis and adaptive security measures, playing a crucial role in strengthening digital defenses
- Organizations will increasingly rely on AI to enhance their cybersecurity defenses, leveraging its advanced threat detection and response capabilities while also addressing the cybersecurity talent gap

> "While AI poses many cybersecurity challenges as it is harnessed by bad actors, it also has huge potential to help organizations improve their cybersecurity posture. Identity access management (IAM) solutions in particular stand to benefit greatly, as AI-powered solutions offer the ability to proactively discover, manage and secure user access far more efficiently than ever before."
>
> *– CEO, Leading MSSP*

Compliance is Top of Mind for CISOs as the Industry Awaits More Regulation

- Government bodies in both the U.S. and Europe are moving forward with efforts to protect critical infrastructure, hold manufacturers accountable for product security and compel private sector companies to disclose material events
- The new and enhanced regulatory environment neces-sitates a proactive approach from boards. By under-standing the requirements, preparing for compliance and balancing cyber risks with growth initiatives, leaders can ensure their companies thrive in this ever-changing digital landscape

> "Dealing with increased regulations are top of mind for many CISOs. Organizations are working to make sure they are prepared, developing incident response plans, and conducting tabletop exercises to ensure that if and when there is a serious incident, they can respond quickly."
>
> *– CIO, Leading SASE Vendor*

FROM DISCUSSIONS WITH SEVERAL CISO'S, SEVERAL KEY THEMES EMERGED:

- **AI Results in Lower Barrier to Entry for Bad Actors:** The rapid evolution of AI, particularly generative AI, will continue to pose challenges and opportunities for CISOs in crafting their strategies
- **AI Poses Tremendous Benefits for Cyber:** Organizations are increasingly incorporating AI into their cybersecurity strategy to bolster digital defenses, leveraging its advanced threat detection capabilities and addressing the talent gap in the industry
- **2024 Will See Increased Regulatory Focus on Cyber:** Private sector companies and critical infrastructure providers will face unprecedented demands for product security, intelligence sharing and transparency on data security

Select Lincoln Cybersecurity M&A & Financing Transactions

2023

sekoia

has received a minority equity investment from

BrightPixel Sonae | BANQUE des TERRITOIRES | BNP PARIBAS ASSET MANAGEMENT | OMNES | Seventure

Capital Raise

2023

ERICOM Be Connected. Be Secure

and its Israeli entity

have been sold to

cradlepoint Connect Beyond

a part of

ERICSSON

Sell-Side

2022

ELLIOTT

has sold

ThreatINSIGHT

a division of

Gigamon®

to

FORTINET

Sell-Side

2022

illusive

has been sold to

proofpoint

a portfolio company of

THOMABRAVO

Sell-Side

2022

zecOps

has been sold to

jamf

Sell-Side

2022

apax

NEW ALPHA ASSET MANAGEMENT

have acquired a majority stake of

MAILINBLACK

Buy-Side

2022

UCF UNIFIED COMPLIANCE FRAMEWORK® The Science of Compliance.®

has been recapitalized by

Allomer | Capital

Sell-Side

2022

TURN // RIVER

has acquired and taken private

tufin

Acquisition Financing
Buy-Side

2022

code42

has sold

CRASHPLAN

to

Mill Point Capital

Sell-Side

2022

A majority stake of

eperi

has been sold to

EQUISTONE

Sell-Side

2021

IK Partners

has acquired

TRUESEC

from

SOBRO

Buy-Side

2021

Advent International GLOBAL PRIVATE EQUITY | EURAZEO

with

planet

have acquired

datatrans.

Buy-Side

2021

WICKS

has sold

SONTIQ

to

TransUnion

Sell-Side

2021

DFLABS CYBER INCIDENTS UNDER CONTROL

has been sold to

sumo logic

Sell-Side

2021

Management and investors

ELRON | arvato BERTELSMANN

have sold

SECUREDTOUCH

to

PingIdentity

Sell-Side

2021

AGARI

has been sold to

helpsystems

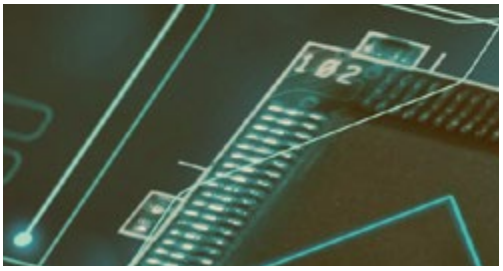
Sell-Side

About Lincoln International

We are trusted investment banking advisors to business owners and senior executives of leading private equity firms and their portfolio companies and to public and privately held companies around the world. Our services include mergers and acquisitions advisory, private funds and capital markets advisory, and valuations and fairness opinions. As one tightly integrated team of more than 950 employees in more than 20 offices in 15 countries, we offer an unobstructed perspective on the global private capital markets, backed by superb execution and a deep commitment to client success. With extensive industry knowledge and relationships, timely market intelligence and strategic insights, we forge deep, productive client relationships that endure for decades. Connect with us to learn more at **www.lincolninternational.com.**

Advisory Services

Mergers & Acquisitions
Capital Advisory
Private Funds Advisory
Valuations & Opinions



Lincoln's Global Technology, Media & Telecom Group

Connected to Clients' Ambitions

Encompassing both physical assets and intellectual property, the technology, media & telecom (TMT) industry has expansive opportunities for investors and entrepreneurs. Our global network of professionals, our strong relationships with industry leaders and our deep expertise in a variety of TMT verticals combine to serve the unique needs of clients capitalizing on change within a sector that is highly integrated into nearly every service and product. Our connections, along with our track record of exceptional results, give us the edge to provide our clients with creative and innovative financial solutions.

Contributors

Chris Brooks
Managing Director | London
+44 20 7632 5248
cbrooks@lincolninternational.com

Alejandro Yu
Director | New York
+1 (212) 277-8108
ayu@lincolninternational.com

Matthieu Rosset
Managing Director | Paris
+33 (0) 1 53 53 17 23
mrosset@lincolninternational.com

Dil Kunnummal
Director | London
+44 20 7632 5232
dkunnummal@lincolninternational.com

Connect with a professional in Lincoln International's Technology, Media & Telecom Group at www.lincolninternational.com/technology