



Houlihan Lokey



Cybersecurity Quarterly Update

THIRD QUARTER 2023

Global Cybersecurity Team

U.S. Cyber Team



Keith Skirbe
Managing Director
Co-Head of U.S. Cyber
San Francisco



Bobby Wolfe
Director
Co-Head of U.S. Cyber
Miami



Joseph Miller
Associate
San Francisco



Rishabh Bansal
Associate
San Francisco



Patrick Wong
Financial Analyst
San Francisco

Capital Markets



Sean Fitzgerald
Managing Director
New York



Chris Hebble
Managing Director
Los Angeles

Global Cyber Reach



Mark Smith
Director
Head of U.K. Cyber
Manchester



Malte Abrams
Managing Director
Head of DACH Cyber
Frankfurt



Sara Napolitano
Managing Director
Head of France Cyber
Paris



Ido Zakai
Managing Director
Head of Tech, Israel
Tel Aviv



Gabrielle Worrall
Vice President
Manchester



Christie Adams
Financial Analyst
Paris



Samuel Pattison
Financial Analyst
Manchester

Financial Sponsors

26

Senior Bankers
Covering

~1,400

Investors

Cybersecurity Technology Expertise



Stephen Lee
Managing Director
Head of Technology and
Cybersecurity
Chicago

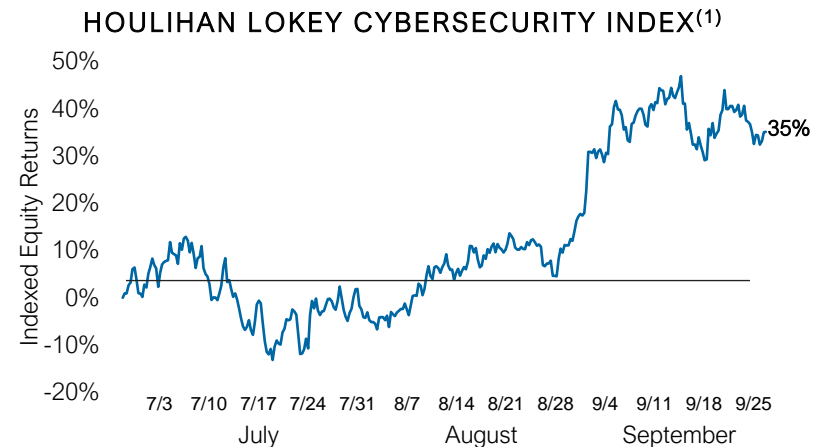


Edouard Viot
Cybersecurity Consultant
Paris

Executive Summary: Q3 2023 in Review

- Private market activity remained depressed in Q3 as M&A and financing deal volume and deal count experienced sustained declines compared to the same period in 2022 and 2021.
- Supported by positive industry trends, investors expect the cybersecurity dealmaking environment to stabilize in early 2024 amid ongoing macroeconomic pressures.
- Q3 '23 M&A deal count fell 17% compared to Q3 '21 but remained roughly in line with Q3 '22 levels, highlighting potential near-term rebound.
- Financing levels in Q3 '23 experienced significant, sustained declines, underscoring investors' continued flight to quality.
- Cybersecurity assets remain attractive long-term investments, driven by heightened demand for innovative, critical solutions.

A Strong Quarter for Public Companies



Q3 2023 Report Themes



AI capabilities in cybersecurity continue to receive positive attention, but cybercriminals are already finding ways to utilize them for their agendas.



Despite new and advanced hacking techniques, ransomware remains the greatest threat and tool for threat actors.



Data breach volumes and associated costs continue their upward surge, garnering more attention in news headlines.



Various government entities are turning their focus to establishing cybersecurity standards.



Despite companies tightening their belts, cybersecurity spending continues to increase and remains a large focus for executives.

M&A Volume Substantially Drops From 2022 Levels

	Q3 '23	VS. Q3 '22	VS. Q3 '21
Volume	\$9.2B ⁽²⁾	↓ (27%)	↓ (48%)
No. of Deals	62	↓ (2%)	↓ (17%)

imperva
\$3.6B

perimeter 81
\$490M

Laminar
\$225M

Financing Levels Continue to Decline

	Q3 '23	VS. Q3 '22	VS. Q3 '21
Volume	\$2.3B	↓ (26%)	↓ (72%)
No. of Deals	99	↓ (55%)	↓ (60%)

onetrust
\$150M

SpyCloud
\$110M

resilience
\$100M

Source: S&P Capital IQ as of September 30, 2023.

(1) Houlihan Lokey Cybersecurity Index includes S, CRWD, ZS, PANW, FTNT, GEN, OKTA, BB, TENB, RPD, CYBR, DARK, QLYS, RSKD, MITK, WITH, FSECURE, AVGO, OTEX, SPLK, FFIV, CHKP, 4704, SWI, SCWX, CGNT, OSPN, and TLS.

(2) Deal volume excludes Cisco's announced acquisition of Splunk.

Case Study: Houlihan Lokey Advises Carlyle on NEVERHACK Acquisition

Transaction Pending

CARLYLE

has agreed to acquire a majority stake in

NEVERHACK

formerly known as **PROPH3CY**

a portfolio company of

IK Partners

Buy-side Advisor

Quick Facts: NEVERHACK

- Headquarters: Guyancourt, France
- Selected Management:
 - CEO: Arthur Bataille
 - CFO: Geoffroy Deguy
- Employees: 600+

Profile

- Carlyle is a global investment firm with deep industry expertise that deploys private capital across its Global Private Equity, Global Private Credit, and Global Investment Solutions business segments.
- NEVERHACK (formerly known as PR0PH3CY), founded in 2021, provides cybersecurity services across the entire cyber services value chain.
- NEVERHACK's cyber services expertise extends across cyber strategy, risk and identity management, audit and configuration, training, and AI tools, serving a highly diverse blue-chip customer base globally.

Rationale

- The Carlyle Europe Technology Partners (CETP) platform will support NEVERHACK's growth as a leading one-stop-shop cybersecurity services business to establish a category leader and consolidator in the cybersecurity sector.
- Carlyle will work with management to continue the company's buy-and-build strategy to gain further scale, broaden its service portfolio, and expand internationally, leveraging its long-standing track record of cybersecurity investments, including in 1E, ManTech, Coalfire, iC Consult, NetMotion, ITRS, Booz Allen Hamilton, and Hack The Box.
- Charles Villet, Managing Director in CETP's investment advisory team, said, "In [NEVERHACK] we recognized a fantastic opportunity to support an attractive and growing consolidation platform in the fragmented cybersecurity sector."

Our Role

- Houlihan Lokey served as the exclusive financial advisor to Carlyle.
- This transaction underscores Houlihan Lokey's strong domain expertise and continued success advising clients in the cybersecurity sector.
- Houlihan Lokey worked collaboratively with Carlyle, assisting it through the transaction.

CARLYLE
NEVERHACK



Table of Contents

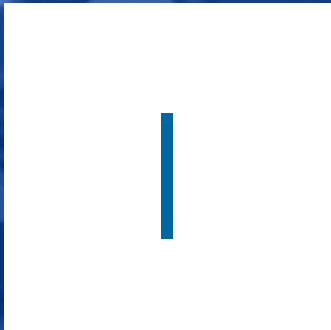
I Perspectives From the Front

II Capital Markets and Trends Update

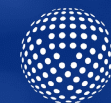
III Conferences and Events

IV About Houlihan Lokey

V Appendix



Perspectives From the Front



Houlihan Lokey



The Only Deep Learning Framework Built Exclusively for Cybersecurity

Deep Instinct prevents malware from entering your organization and blocks malicious code from being written to disk using deep learning technology specifically built for cybersecurity use cases. Their platform protects your data, reduces SOC burnout, and enables innovation.

What Security Operations Professionals Are Focused On

Generative AI: Business Friend or Foe?



Generative AI (GenAI) tools are commonly used and have positive effects on productivity and employee morale, but senior security professionals express concerns about their disruptive potential and potential vulnerabilities to attacks. These concerns mainly revolve around issues such as privacy, undetectable phishing attacks, and an increase in the frequency and speed of cyber-attacks.

Ransomware: As New Vulnerabilities Emerge, an Old Threat Remains a Challenge



Ransomware is increasingly perceived as the greatest threat to data security, with a growing C-suite concern, leading to a shift in security strategies and a rise in organizations willing to pay ransoms for data recovery.

Mounting Security Team Stress: A Call to Change the Status Quo



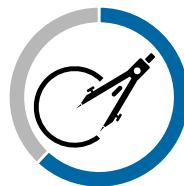
Security professionals are experiencing increased stress levels, primarily due to staffing and resource limitations, leading to a significant likelihood of job turnover. The strain caused by false positives from outdated cybersecurity tools highlights the demand for improved solutions, with a growing emphasis on prevention rather than reaction in the industry.



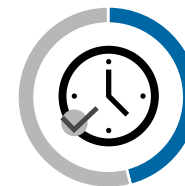
“ In this new era of generative AI, the only way to combat emerging AI threats is by using advanced AI—one that can prevent and predict unknown threats. Relying on antiquated tools like EDR is the equivalent of fighting a five-alarm fire with a garden hose.

Assuming breach has been an accepted stance but the belief that EDR can get out ahead of threats is simply not true. A shift toward predictive prevention for data security is required to remain ahead of vulnerabilities, limit false positives, and alleviate security team stress.

Lane Bess, CEO, Deep Instinct



62% of security professionals admit that ransomware is the No. 1 C-suite concern, up from 44% in 2022.



46% of senior security professionals view GenAI as a disruptive threat, believing GenAI will increase their organizations' vulnerability to attacks.



55% of security professionals say their stress levels have increased, with the top reason being staffing and resource limitations (42%).

Critical Takeaways

- Top Chief Information Security Officers (CISOs) are continuing to prioritize their cyber postures regardless of macroeconomic conditions; the investment is paying off in the form of fewer and less costly breaches, more efficient security operations, and faster growth/productivity enabled by the ability to utilize new technologies—such as AI—with confidence in security.
- The number of attack vectors and the cost of breaches are continuing to proliferate, requiring a continuous evolution of cyber risk management programs being driven by technology modernization and streamlined cyber tech stacks.
- Consistency of cyber investment despite macro tightening and uncertainty, the blurring of espionage and cybercrime, threats introduced by GenAI, and the adoption of governmental cyber regulations are the major disruptive shifts in focus.

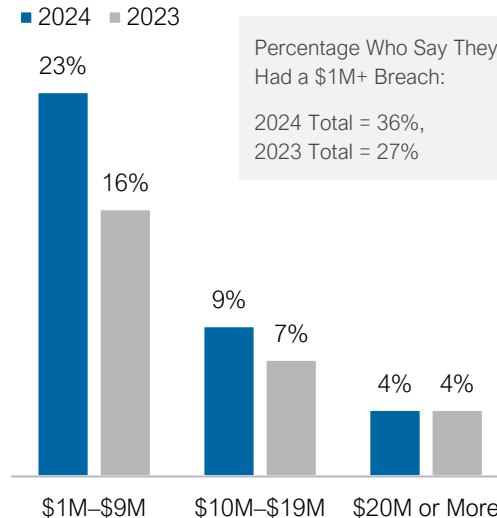
Cloud Migration and Remote Access Have Created Headaches for CISOs

Over the next 12 months, which of the following cyberthreats is your organization most concerned about?



The Cost of Data Breaches Continue to Rise

Cost of the most damaging breach in the past three years:



Top Performers vs. the Rest

Businesses are reinventing themselves and senior executives are becoming more innovative in the way they secure their organizations. There is a clear pattern emerging on what they are doing differently, their opinions and the results of their programs:

Top 5% Are:



6x more likely to have already implemented transformative cybersecurity initiatives from which they are realizing benefits.



5x more likely to be very satisfied with their current cyber technology capabilities.



4x more likely to be continually updating their risk management plans to mitigate cloud risks.



9x more likely to be mature in their cyber resilience practices.

Top 5% Are More Likely To:



Invest more into cyber budget, with **85% increasing their cyber budget in 2024** (vs. 79% overall), of which 19% are increasing cyber budget in 2024 by 15% or more, compared to 10% overall.



Say their **most damaging cyber breach** in the past three years cost them less than \$100K (28% vs. 19% overall).



Strongly agree that their **organizations will develop new lines of business using GenAI** (49% vs. 33% overall).



Plan to deploy GenAI tools for cyber defense (44% vs. 27%).



Disagree that “GenAI will lead to a catastrophic cyber-attack” (33% vs. 22% overall).

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Cyber Research Summary

2023 Prediction Tracking

Data Breaches



SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

The SEC adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose, on an annual basis, material information regarding their cybersecurity risk management, strategy, and governance.

Highlights of New Regulations

1

SEC Mandates Disclosure of Cybersecurity

The SEC's new rules compel public companies and foreign private issuers to disclose critical cybersecurity incidents and management strategies, underlining the growing importance of cybersecurity transparency in business.

2

SEC Drops Requirement to Disclose Individual Board Members' Cybersecurity Qualifications in Filings

The SEC removed the proposed requirements to identify individual board of director members with expertise in cybersecurity matters and to disclose their qualifications and experience in relevant filings but retained the requirement to identify relevant expertise of cybersecurity management.

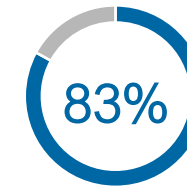
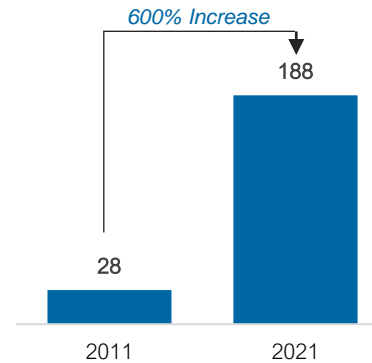
3

Regulations to Take Effect in 2024

The phased implementation of these regulations allows businesses to adapt to the new disclosure requirements, reflecting the SEC's commitment to enhancing cybersecurity reporting while providing companies with time to adjust.

Metrics the SEC Is Tracking

Data Breaches in the U.S.



of organizations in 2022 experienced **more than one data breach**.

In 2022, the average cost of a data breach in the U.S. was:

\$9.44 Million

Overall, some estimates on the economy-wide total costs run as high as trillions of dollars per year in the U.S. alone.



Currently, in the absence of specific disclosure requirements, companies can cherry-pick disclosures of their cybersecurity risk management processes, that is, if they disclose at all. By clarifying what companies must disclose, the rule will provide investors with more certainty and easier comparability. This will reduce the risk of adverse selection, and the potential mispricing of a company.

Beyond the clear benefits to investors, the rule will also have broader, indirect benefits. For example, more timely reporting of cyber incidents can serve as an alert to companies in the same sector that malign actors are launching cyber-attacks. Such companies could have more time to raise their cyber defenses and to mitigate any potential damage.

Jaime Lizárraga, SEC Commissioner



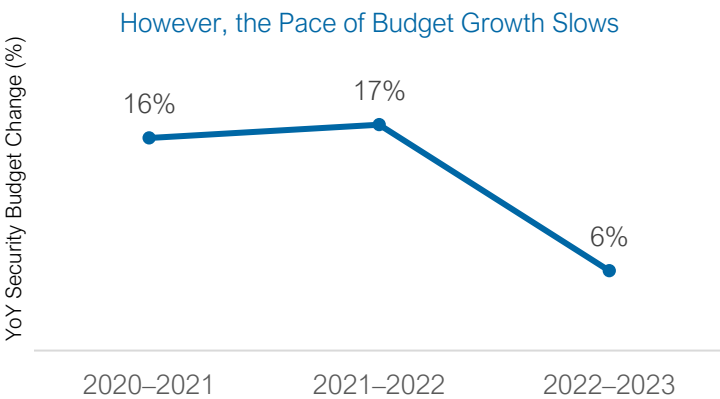
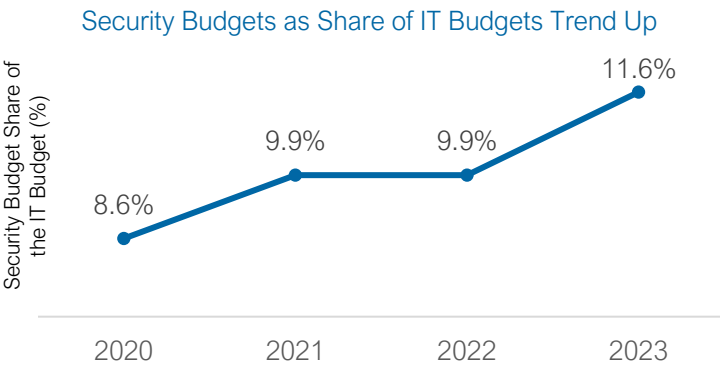
Cyber Research Summary

2023 Prediction Tracking

Data Breaches

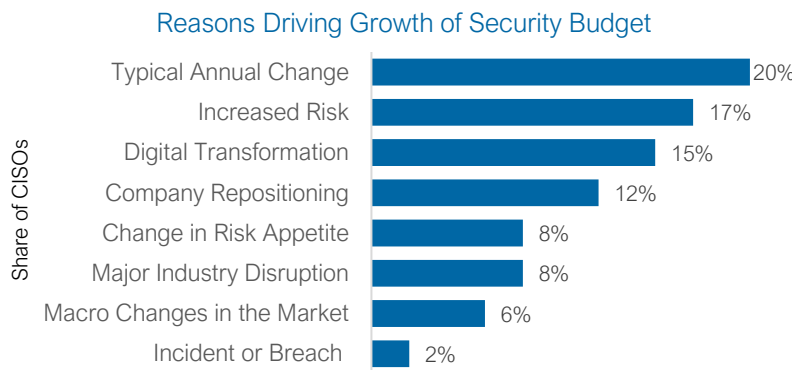
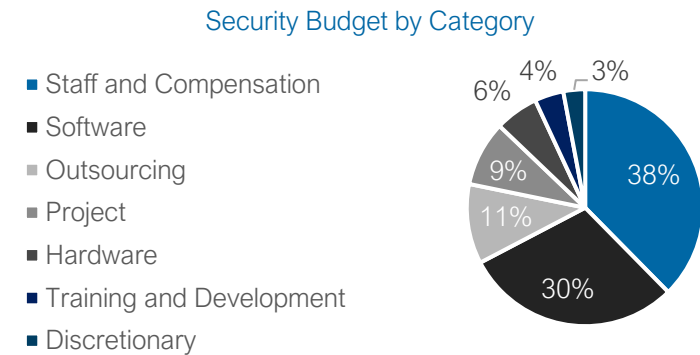
Security Budget Annual Growth Shows Restraint

Over the past year, global businesses significantly reduced their investments in enterprise technology due to concerns about the uncertain financial climate, potential recession, and rising inflation. Despite these challenges, security budgets continued to increase, although not as rapidly as in previous years.



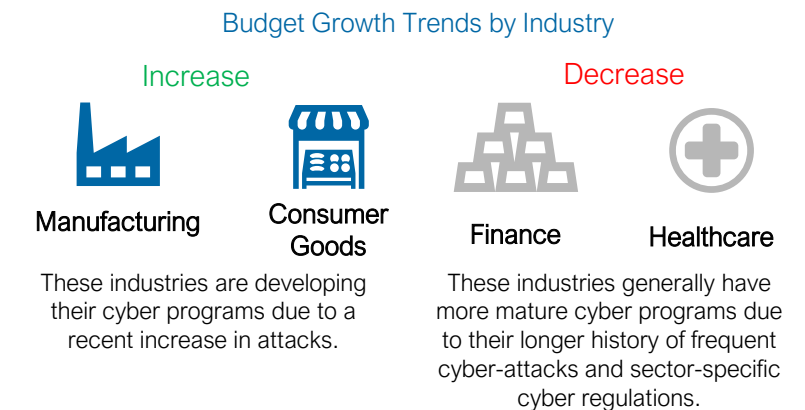
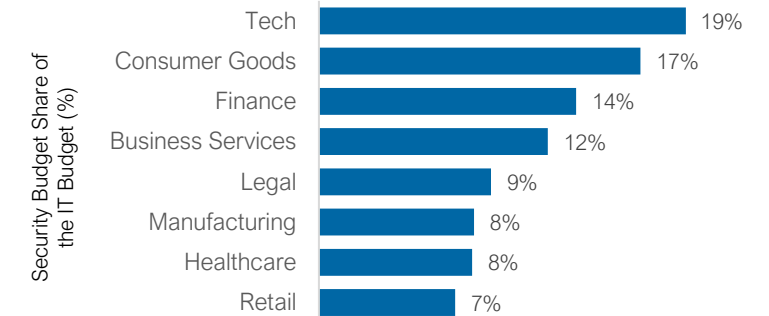
Staff and Compensation Claims Largest Budget Share

CISOs clarify that they possess an adequate array of tools but are lacking the necessary workforce to fully leverage them. The allocation for staff and compensation continues to be the largest category of security expenditure, accounting for 38% of the total security budget.



The Adoption Cycle Varies by Industry

The variability in budgeting by industry reflects differences in risk profiles, cyberthreat levels, and cyber program maturity. Laggards have been targeted as vulnerable parties, while early adopters have been able to realize efficiencies.



Greylock: Securing AI, the Next Platform Opportunity in Cybersecurity

Cyber Research Summary

2023 Prediction Tracking

Data Breaches

Critical Takeaways

- AI and foundation models are a primary focus for CISOs and CIOs in both large enterprises and startups, representing a significant shift in software development.
- Startups that bridge the gap between AI and security are presented with significant opportunities to address the growing demand for visibility, governance, and auditability in AI-based solutions.
- Inaugural AI security use cases address a range of critical concerns, from data provenance and AI agent identities to model vulnerabilities, MLSecOps, and protection against prompt injection, indirect attacks, and model theft.

Security Professionals Need to Be Aware of AI Impacts and Potentially Malicious Use Cases

Posture



- 1 Data Provenance and Policies:** Organizations must adhere to data storage, retention, and usage regulations across regions. They need to track data origin, sensitivity, bias, and potential legal risks like copyright or open-source licenses.
- 2 MLSecOps and Model Testing:** Embedding code in AI pipelines enables vulnerability detection, model BOM creation for tracing and audits, and pre-production stress tests to assess model robustness against various data types and common attacks.
- 3 AI Agent Identities:** As AI agents enter the enterprise, organizations must govern their access and functions, potentially surpassing RPA security due to their unpredictability and increased capabilities.
- 4 Model Registries/Toolchain Vulnerabilities and Supply Chain Risk:** Tools are vital for uncovering flaws in OSS models and toolchains, like the PyTorch vulnerability. Third-party dependencies in upstream services pose additional risks, such as the Redis cache bug affecting ChatGPT. Safetensors offer a secure substitute for pickle files in handling model weights to prevent arbitrary code execution during unloading.

Detection and Response



- 1 Indirect Prompt Attacks:** Systems with multiple components can introduce risks. They might call webpages with hidden comments, establish compromised connections, or lead to permission escalation. Treating these systems as arbitrary code execution engines is risky.
- 2 Data Poisoning Prevention:** Implement safeguards to thwart malicious, low-quality, or unsupported data input by attackers, preventing model exploitation or performance degradation.
- 3 Prompt Injection:** Malicious prompts can be employed to try to breach the system, gain unauthorized access, or pilfer sensitive data. Recent research has explored the systematic generation of adversarial prompts using both greedy and gradient search methods.
- 4 Response Assessment:** Failing to control incorrect or toxic responses poses risks, potentially harming a company's reputation. Legal issues like PII and copyright concerns are also at play. This challenge stems from the transition from deterministic software outputs to stochastic ones.

Our Predictions

MFA Bypass Techniques



- As multifactor authentication (MFA) is more widely adopted, new MFA vulnerabilities and bypass techniques are expected in 2023.
- The most common way cybercriminals will sidestep these solutions is through smart social engineering and MFA push notification impersonations.

State-Sponsored Attacks



- State-sponsored crime is a heightened threat compared with previous years, as Russia, China, and Iran are all currently involved in conflict.
- These and other nation-state actors will use cybersecurity tactics to advance their objectives as part of both outright conflict and covert operations.

What Happened

- MGM fell victim to a significant cyber-attack that exploited an employee's stolen credentials and bypassed multi-factor authentication through a brief phone call with the help desk, resulting in an estimated loss of more than \$80 million.
- Attackers use six main MFA bypass techniques, which have all grown more complex, resulting in **more than 1.24 million MFA bypass attacks recorded every day**.
 - MFA Fatigue
 - MFA Flood
 - Attacker in the Middle
 - MFA Reset
 - SIM Swapping
 - Oktapus Style

- **This year, more than 120 countries and territories** experienced state-sponsored cyberthreat activity against organizations, with Ukraine, the United States, and Israel being the most targeted.
- Hacktivists, politically motivated hackers, are already making their mark on the Israel-Hamas conflict. With both pro-Palestinian and pro-Israel groups involved, news outlets such as *The Jerusalem Post*, **emergency alert services such as RedAlert, and even airports have experienced disruptions from cyber-attacks**. As the conflict continues to unfold, it is expected that more state-sponsored hacker groups will join in to further their own agendas.

What We Did Not Predict: Crypto-Based Crime Revenue Down 77% vs. 2022

Despite cryptocurrency asset prices increasing, which usually invites bad actors, 2023 is seeing a drastic decrease in crypto-related scams.



“While we are encouraged by the disappearance of the two scams [VidiLook and Chia Tai], which could be due to law enforcement and pressure, this is a fragile trend. We are on the lookout on what the next big scam might be, so we can highlight these to the private and public sectors.

Jacqueline Burns Koven, Chainalysis



- The sharp decline in cryptocurrency scam revenue in 2023 is primarily due to the sudden exit scams of two major schemes: VidiLook and Chia Tai Tianqing Pharmaceutical Financial Management. VidiLook, in particular, defrauded users of more than \$120 million in a short time by offering cryptocurrency rewards for watching ads and staking.
- Despite overall scams decreasing, Ransomware attacks have surged in 2023, with attackers extorting at least \$449.1 million through June. **If this pace continues, they could reach \$898.6 million in extortions, second only to 2021**. This resurgence is driven by “big game hunting” and a rise in smaller attacks. Payment sizes have grown at both ends, with low-level ransomware-as-a-service strains targeting smaller targets and sophisticated strains aiming at larger organizations.

Cyber Research Summary

Breach Overview

Company Description: U.S. cleaning product manufacturer

Date of Breach: August 2023

What Happened: Cyber-attack on Clorox damaged parts of its IT infrastructure, forcing it to temporarily take certain systems offline and switch to processing orders manually; the attack led to widespread disruption of its production capabilities resulting in product shortages

Outcome of Breach: Clorox expects net sales to decrease 23%–28% and estimates its gross margin for the quarter will be down from the year-ago period.

Key Stats⁽¹⁾

~35¢–75¢

Expected Loss per Share in the Quarter Ended on September 30

23%–28%

Expected Fall in Net Sales From a Year Earlier

40¢

Projected Loss per Share on an Adjusted Basis

\$25M

Cost of Hiring Forensic Investigators and Legal and Technology Help

2023 Prediction Tracking

Attack Methodology and Rationale

As reported by Bloomberg, the European and U.S. group of hackers called Scattered Spider is suspected of being tied to the August attack on Clorox.



Clorox has not provided details regarding how the suspected hackers managed to access its IT network, nor has the company disclosed what (if any) corporate information or customer data was exfiltrated.

Expert Opinions and Commentary



“Details into this incident are still emerging, so it isn’t clear what type of attack Clorox is facing. However, based on the information available, the company has taken certain systems offline to contain the incident. This could indicate the attack was ransomware, and Clorox is trying to prevent the malware from spreading onto other systems.”

— Jordan Schroeder, Managing CISO at Barrier Networks

Cybersecurity experts repeatedly state the importance of risk assessments and understanding that supply chain attacks are just as potentially deadly as attacks targeting plants and OT directly.

Data Breaches

The Outcome

- The cyber-attack will have a material impact on the financial performance of Clorox due to disrupted business operations.
- Currently, Clorox has spent \$25 million to respond to a suspected ransomware attack, including hiring forensic investigators and legal and technology help, and expects more cyber expenses to arise in 2024.
- Clorox implemented workarounds for certain offline operations in order to continue servicing its customers and engaged third-party cybersecurity experts to support its investigation and recovery efforts.
- Clorox expects operational impacts from the cyber-attack to continue into Q2 '24, though the majority of order processing operations have returned to automated processes.
- The company will continue to assess the impact of the attack on the remainder of FY 2024.

Key Takeaways⁽¹⁾



Robust Business Continuity Plans (BCP)

The company’s BCP was not complete and did not account for this disruption and Clorox may have failed to exercise and test its BCP. A good BCP should have a good indication of a recovery time objective (RTO). RTOs are typically measured in hours, potentially days. It is very rare that an RTO will be longer than a month.



Enhanced Cybersecurity Hygiene

Pivotal aspects of cybersecurity hygiene include contingency plans to limit the damage in the event of an IT system compromise and the need for data backups and redundancy to aid in speedy recovery.

Data Breaches: MGM Resorts

Cyber Research Summary

Breach Overview

Company Description: Hospitality and entertainment company operating resorts globally

Date of Breach: September 2023

What Happened:

Scattered Spider and AlphV/BlackCat made a cyber-attack on MGM exposing personal information of the guests, including name, contact information, gender, date of birth, driver's license, passport, and Social Security number; additionally, significant customer service was impacted (access to rooms, elevators, kiosks, gaming consoles, etc.)

Outcome of Breach: Hotel occupancies fell to 88% during the month of September, compared with 93% the prior year

Key Stats⁽¹⁾

~\$80M
Lost Revenue Due to Operational Disruptions

\$10M
Costs for Technology Consultants, Legal Fees, and Other Third-Party Advisors

6%
Decline in September Hotel Occupancies Compared to Prior Year

36
Hours of IT Downtime

2023 Prediction Tracking

Attack Methodology and Rationale



European and U.S. hacker groups, including Scattered Spider and AlphV/BlackCat, are believed to be behind the cyber-attack, allowing them to gain customers' personal data.



They were able to launch the attack against MGM through a method known as voice phishing or "vishing," according to the site vx-underground. The group allegedly targeted an MGM employee and then contacted the company help desk to bypass MFA requirements, according to the site.

Expert Opinions and Commentary



Lisa Plaggemier, Executive Director at the nonprofit National Cybersecurity Alliance, called MGM's decision to shut down vulnerable systems to prevent intrusion a positive step but said it highlighted "significant" security gaps and an urgent need for substantial investment in employee training and cybersecurity. The risk, she said, is "downtime and financial losses."

Hospitality has always been a prime target for cybercriminals. This sector holds a treasure trove of personal data, including names, passports, addresses, and credit card numbers, that are sold for profit.

Data Breaches

The Outcome

The breach led to potential financial losses, reputational damage, and legal implications for MGM.



MGM is facing class action litigation in two separate lawsuits filed in U.S. District Court in Nevada in connection with the cyber-attack launched against the company in September 2023. The suits allege the company was negligent and gained unjust enrichment for failing to protect the personal data of MGM customers from the alleged social engineering attack.



This incident highlights the importance of segmenting the network architecture.⁽¹⁾

Key Takeaways⁽¹⁾

Defense-in-Depth

Harden cybersecurity defenses through automated moving target defense (AMTD) as part of a robust defense-in-depth strategy. AMTD introduces added complexity and attack cost for the threat actor, thereby providing an effective deterrent and barrier against ransomware attacks.

IR Framework and Response Alignment

IR framework and response practices must align practically with company operations and steps enacted to ensure employees are connected with such practices. This ensures a natural response to incidents where actions are planned, thoughtful, and properly executed.

Cyber Research Summary

Breach Overview

Company Description: Personal genomics and biotechnology company

Date of Breach: October 2023

What Happened: 23andMe confirmed that data from a subset of its users had been compromised; the company said its systems were not breached and that attackers gathered the data by guessing the login credentials of a group of users and then scraping more people's information from a feature known as DNA Relatives

Outcome of the breach: Sensitive personal data was leaked, and attackers were selling the profiles for \$1–\$10 per account

Key Stats⁽¹⁾



1+ Million
Data Points Exposed



\$1–\$10
Amount Hackers Charged per Account for the Data Leaked

2023 Prediction Tracking

Attack Methodology and Rationale

A group of hackers executed a credential-stuffing attack against the company: using credentials stolen from another site to gain unauthorized access to individual 23andMe accounts. The hackers claimed the sample contained 1 million data points belonging to Ashkenazi Jews.



Users can opt into 23andMe's DNA Relatives feature, which allows users to find and connect with other users who have opted into that feature. A single user could see thousands of genetic matches; hackers likely scraped the list of people with Ashkenazi heritage by accessing accounts that use that feature.

Expert Opinions and Commentary



"When data is shared relating to ethnic, national, political or other groups, sometimes it's because those groups have been specifically targeted, but sometimes it's because the person sharing the data thinks it'll make reputation-boosting headlines. This incident really highlights the risks associated with DNA databases. The fact that accounts had reportedly opted into the 'DNA Relatives' feature is particularly concerning as it could potentially result in extremely sensitive information becoming public."

— Brett Callow, Threat Analyst at Emsisoft

With such platforms come all the data privacy and security issues that have plagued traditional social networks, including issues related to data centralization and scraping.

Data Breaches

The Outcome

- As per the reports, the attackers were offering the data profiles for purchase with profiles being sold for \$1–\$10 per account.
- However, an investigation into the legitimacy of the data is ongoing, though the leaked data is consistent with an internal company situation in which some accounts were exposed and used to access more data through 23andMe's DNA Relatives feature.
- This incident raises broader questions about keeping sensitive genetic information safe and the risks of making it available in services that are designed like social networks to facilitate sharing.
- 23andMe is already facing a class action lawsuit that alleges negligence, breach of implied contract, and invasion of privacy. The lawsuit argues that the company attempts to blame the threat actors without giving users adequate knowledge of how the breach occurred and if the threat has been contained.

Key Takeaways^(1,2)

Need of Strong Privacy Laws

There is a need for privacy laws attuned to how the information economy works. Providing consent on behalf of others—as 23andMe users did when they clicked "I agree"—would be illegitimate under any meaningful notion of consent. To contain group data harms like those produced in this hack, we need substantive rules about what companies can and can't do.



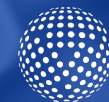
Importance of Choosing a Unique, Strong Password

This incident highlighted the importance of choosing passwords they've never used on other sites, as well as turning on two-factor authentication.





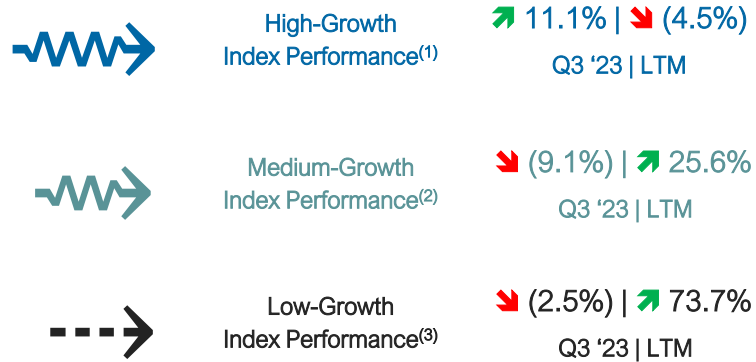
Capital Markets and Trends Update



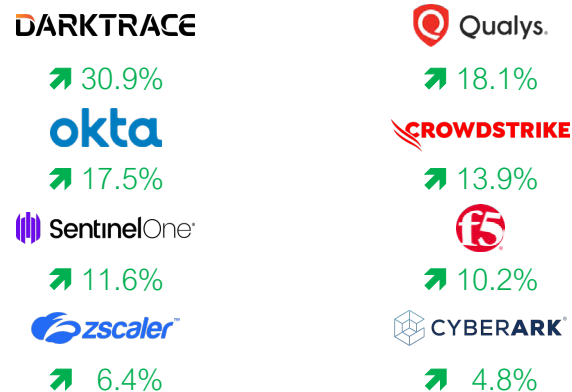
Cybersecurity Dashboard

Public Market Environment

Trailing 12-Month (LTM) Performance Remains Robust
Despite Dampened Q3 Results

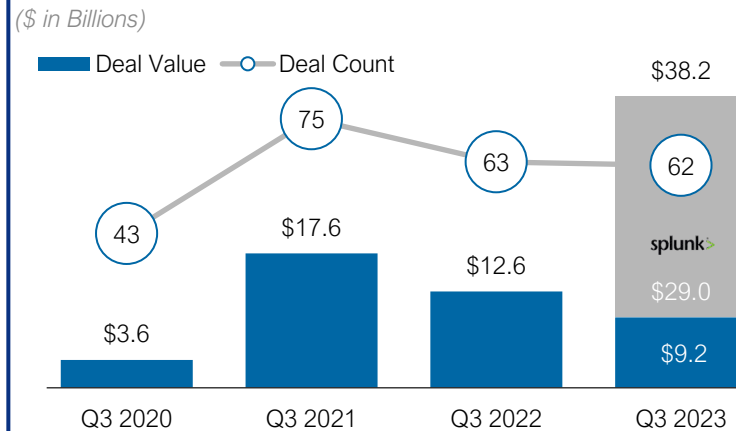


Selected Cybersecurity Performance Q3 2023



M&A Environment

Despite Sustained Take-Private Activity and Positive Industry Trends Providing Upside Support, M&A Activity Remains Depressed



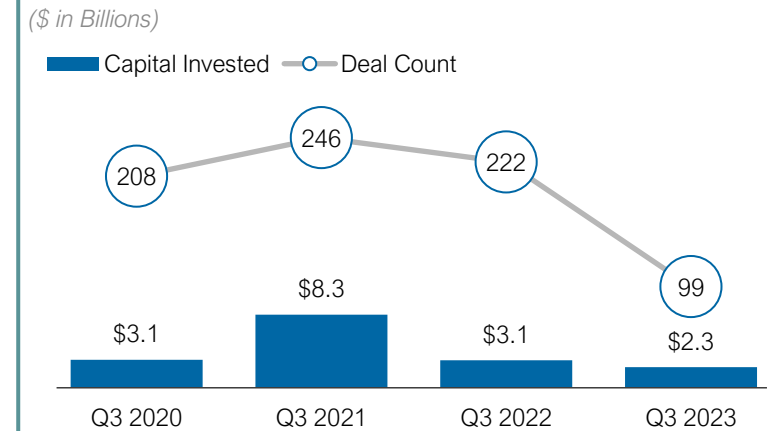
Selected Q3 Transactions

(\$ in Millions)

Ann. Date	Acquirer	Target	EV	EV/Rev
Sep-20	CISCO	splunk	\$29,005	7.5x
Sep-07	tenable	ermetic	\$265	26.5x
Aug-10	CHECK POINT	perimeter 81	\$490	24.5x
Jul-25	THALES	imperva	\$3,600	7.2x
Jul-10	TPG	Forcepoint	\$2,450 ⁽⁴⁾	7.5x ⁽⁴⁾

Private Funding Environment

Private Funding Downturn Persists as Investors Hold Out for Value Opportunities in a Volatile Financing Environment



Selected Q3 Financings

(\$ in Millions)

Ann. Date	Investor	Target	Amount	Val.
Sep-19	Lightspeed	CATO NETWORKS	\$238	\$3,000
Sep-18	BlackRock KOCH DISRUPTIVE TECHNOLOGIES	DRAGOS	\$274	\$1,974
Aug-16	RIVERWOOD CAPITAL	SpyCloud	\$110	\$410
Aug-07	[intact] VENTURES	resilience	\$100	\$950
Jul-24	generation	onetrust	\$150	\$4,500

Source: S&P Capital IQ as of September 30, 2023.

(1) High-growth index includes CRWD, ZS, and S.

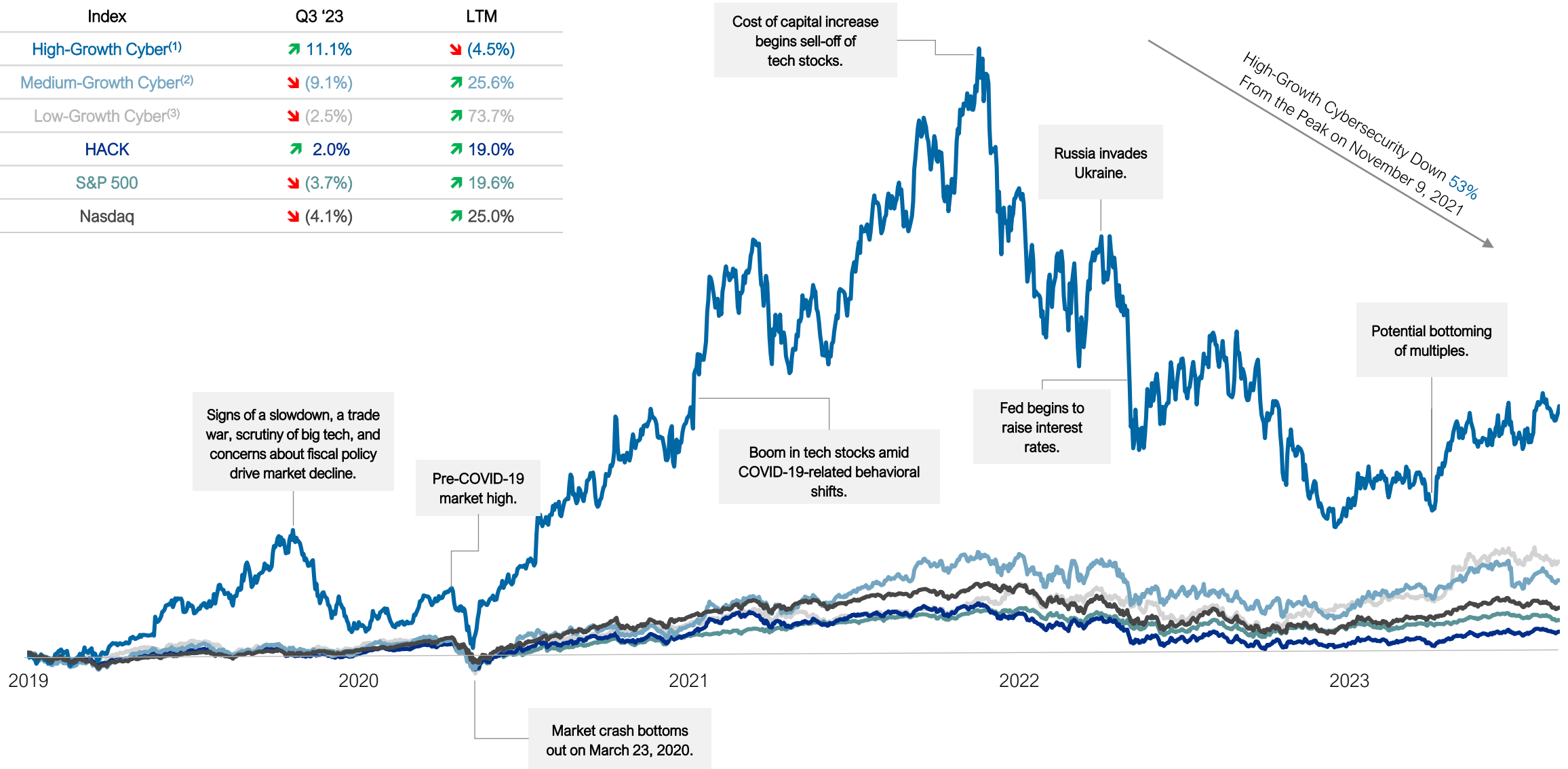
(2) Medium-growth index includes PANW, FTNT, GEN, OKTA, CYBR, QLYS, TENB, RPD, DARK, BB, FSECURE, MITK, and RSKD.

(3) Low-growth index includes AVGO, SPLK, OTEX, CHKP, FFIV, 4704, SWI, SCWX, OSPN, CGNT, WITH, and TLS.

(4) Implied enterprise value and revenue multiple per Wall Street estimates.

Some Segments of Cybersecurity Posted Strong Quarter and Outpaced Broader Indices

Index	Q3 '23	LTM
High-Growth Cyber ⁽¹⁾	↗ 11.1%	↘ (4.5%)
Medium-Growth Cyber ⁽²⁾	↘ (9.1%)	↗ 25.6%
Low-Growth Cyber ⁽³⁾	↘ (2.5%)	↗ 73.7%
HACK	↗ 2.0%	↗ 19.0%
S&P 500	↘ (3.7%)	↗ 19.6%
Nasdaq	↘ (4.1%)	↗ 25.0%



Source: S&P Capital IQ as of September 30, 2023.

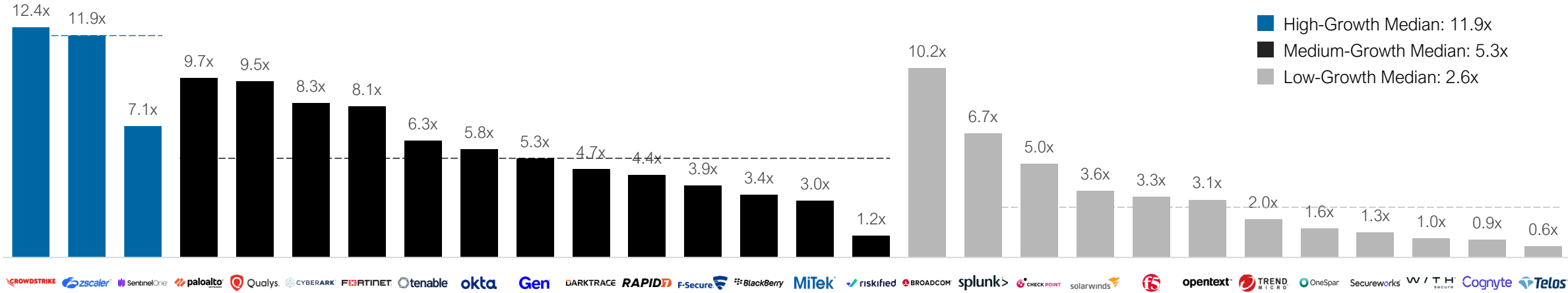
(1) High-growth cybersecurity includes S, CRWD, and ZS.

(2) Medium-growth cybersecurity includes PANW, FTNT, QLYS, CYBR, TENB, GEN, OKTA, RPD, DARK, MITK, BB, FSECURE, and RSKD.

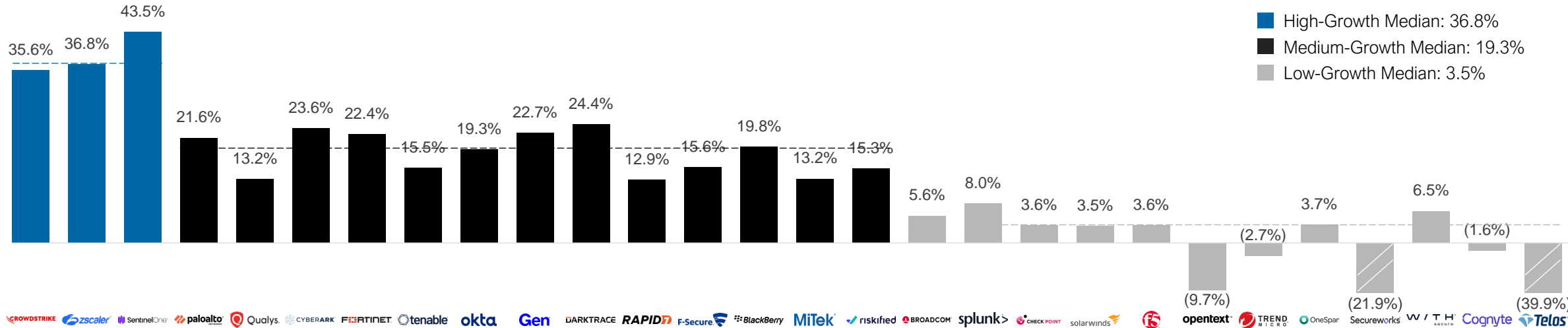
(3) Low-growth cybersecurity includes AVGO, SPLK, SCWX, TLS, CGNT, CHKP, 4704, SWI, FFIV, OTEX, WITH, and OSPN.

Public Company Benchmarking: Cybersecurity Software

EV/2023E Revenue



CY 2022A-2023E Revenue Growth



Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of September 30, 2023. Notes: All financials are calendarized to a December year-end. Sorted by EV/2023E revenue.

Public Investors Remain Focused on Growth and Profitability

Low Revenue Growth Rate	Medium Revenue Growth Rate	High Revenue Growth Rate
-------------------------	----------------------------	--------------------------

Mean: (3%) | 3.3x
 Median: 4% | 2.6x

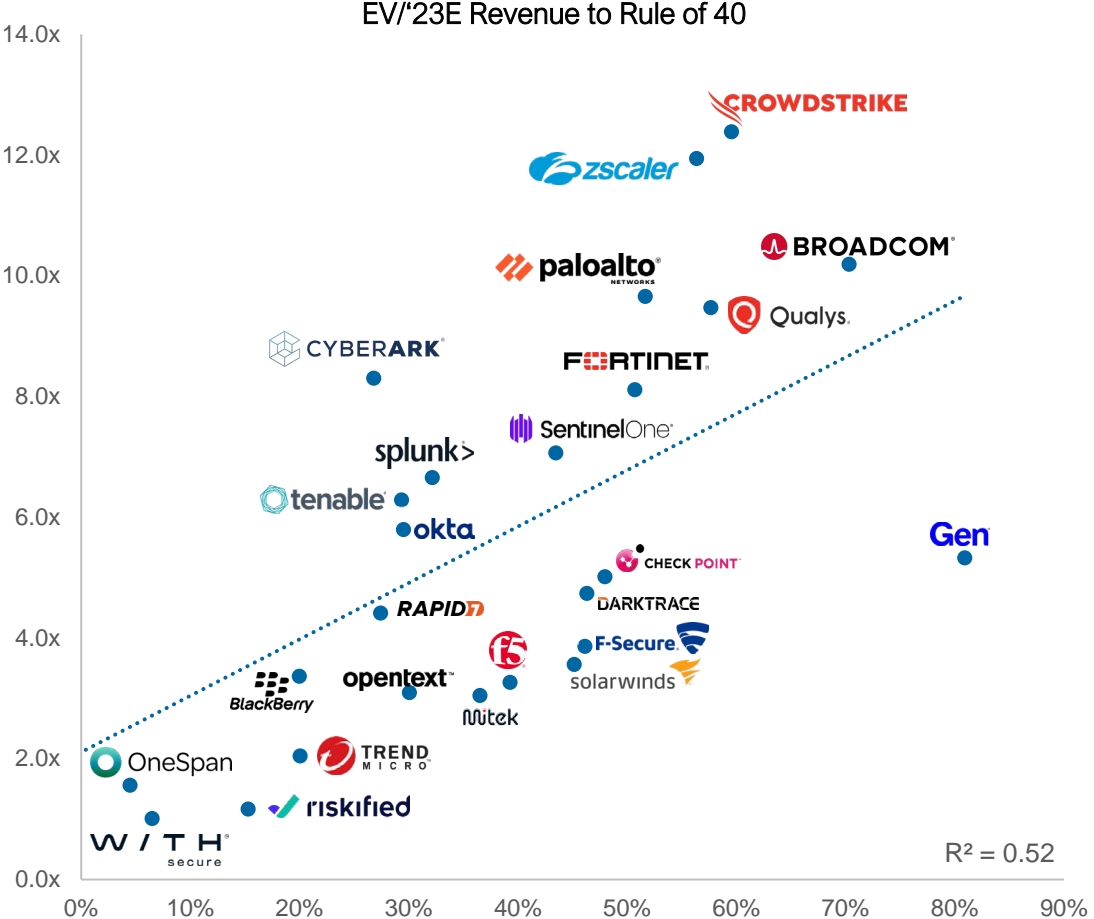
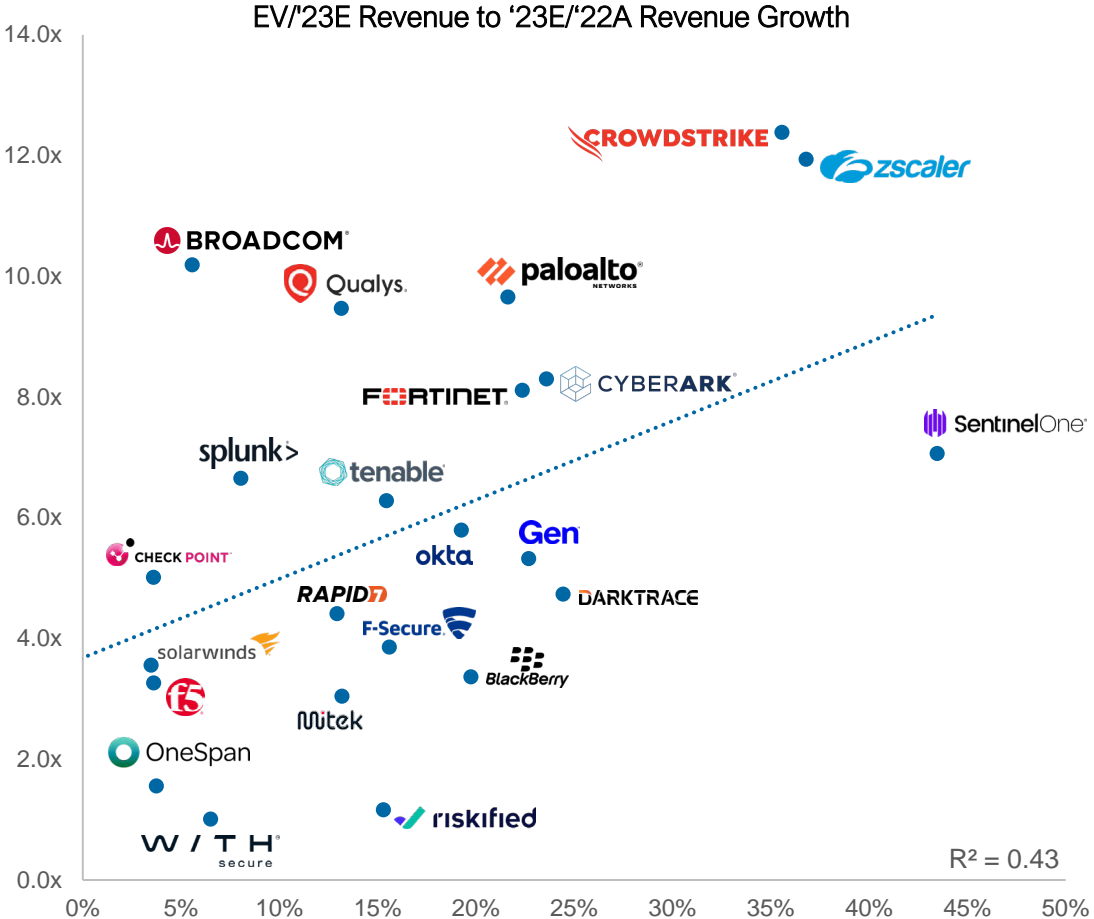
Mean: 18% | 5.7x
 Median: 19% | 5.3x

Mean: 39% | 10.5x
 Median: 37% | 11.9x

Below "Rule of 40"	Above "Rule of 40"
--------------------	--------------------

Mean: 4% | 3.3x
 Median: 7% | 3.1x

Mean: 21% | 7.6x
 Median: 22% | 7.6x

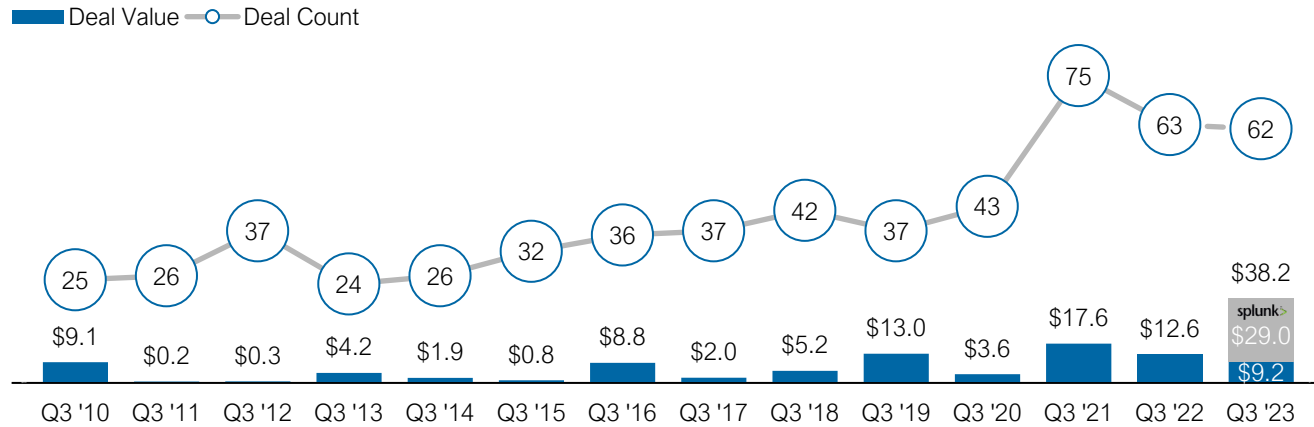


Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of September 30, 2023. Notes: All financials are calendarized to a December year-end. Companies with negative values for revenue growth are included in the calculation for R² but are not included in the charts.

Cybersecurity M&A Activity

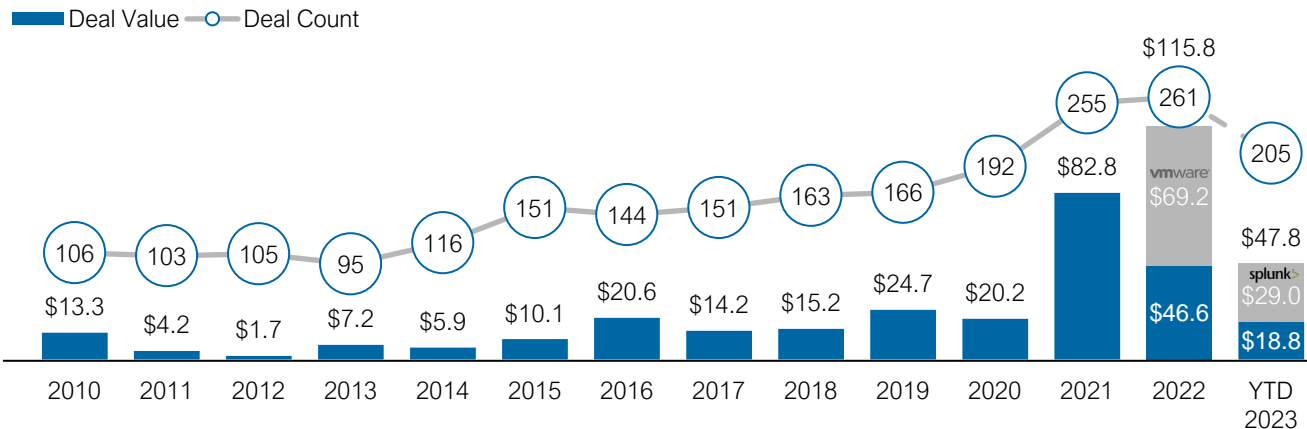
Historical Q3 M&A Summary

(\$ in Billions)



Annual M&A Summary

(\$ in Billions)



Selected M&A Transactions

(\$ in Millions)

Ann. Date	Acquirer	Target	EV	EV/Rev
Sep-20	CISCO	splunk	\$29,005	7.5x
Sep-07	tenable	ermetic	\$265	26.5x
Sep-05	First Advantage	InfiniteID	\$41	NA
Aug-30	SailPoint	OSIRIUM	\$6	2.8x
Aug-23	PARSONS	SEALINGTECH	\$175	NA
Aug-10	CHECK POINT	perimeter 81	\$490	24.5x
Aug-08	rubrik	Laminar	\$225	NA
Aug-02	FRANCISCO PARTNERS	blanco technology group	\$207	4.3x
Jul-25	THALES	imperva	\$3,600	7.2x
Jul-13	CISCO	DORT	NA	NA
Jul-10	SpireCapital	COBWEBS TECHNOLOGIES	\$200	NA
Jul-10	TPG	Forcepoint	\$2,450 ⁽¹⁾	7.5x ⁽¹⁾

Sources: S&P Capital IQ, PitchBook, 451 Research as of September 30, 2023.

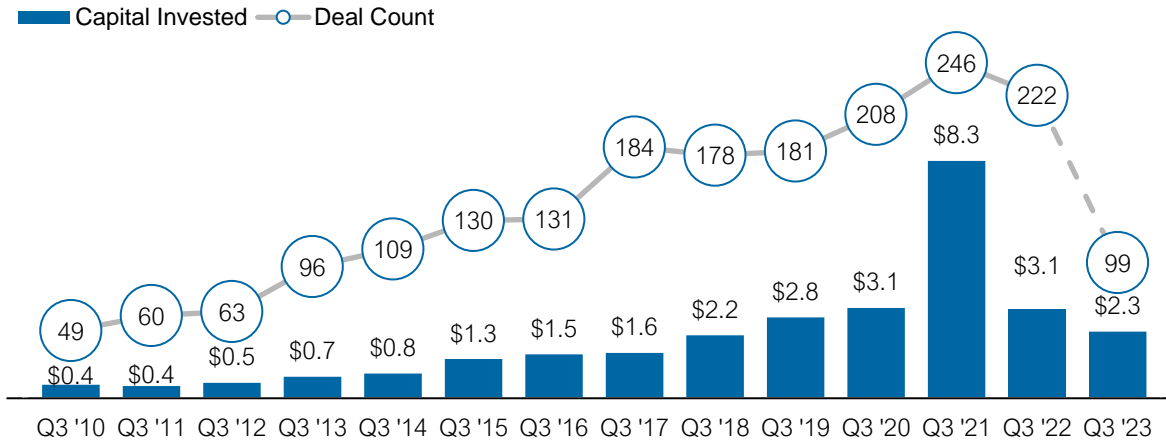
Notes: NA indicates not available; NM indicates not meaningful. 2022 M&A deal volume includes Broadcom's acquisition of VMware. 2023 M&A deal volume includes Cisco's acquisition of Splunk.

(1) Implied enterprise value and revenue multiple per Wall Street estimates.

Cybersecurity Financing Activity

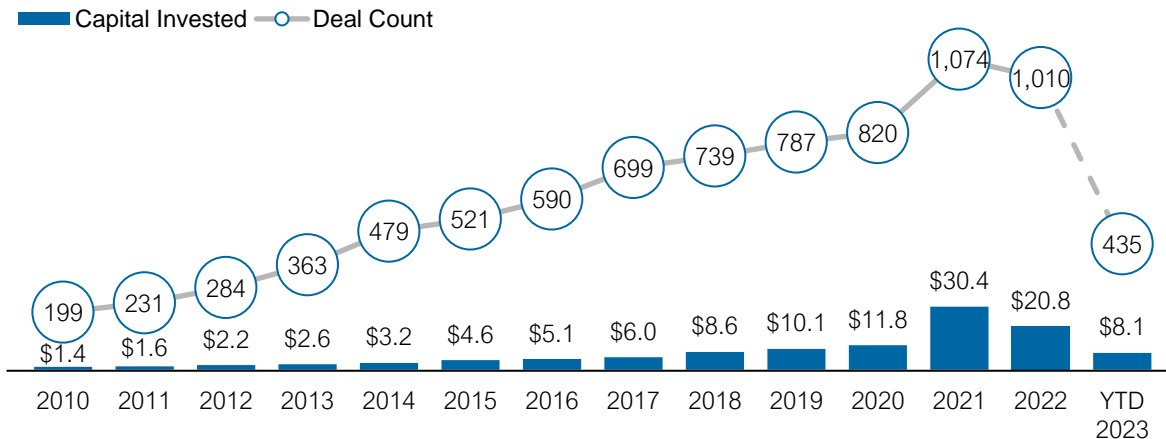
Historical Q3 Financing Summary

(\$ in Billions)



Annual Financing Summary

(\$ in Billions)



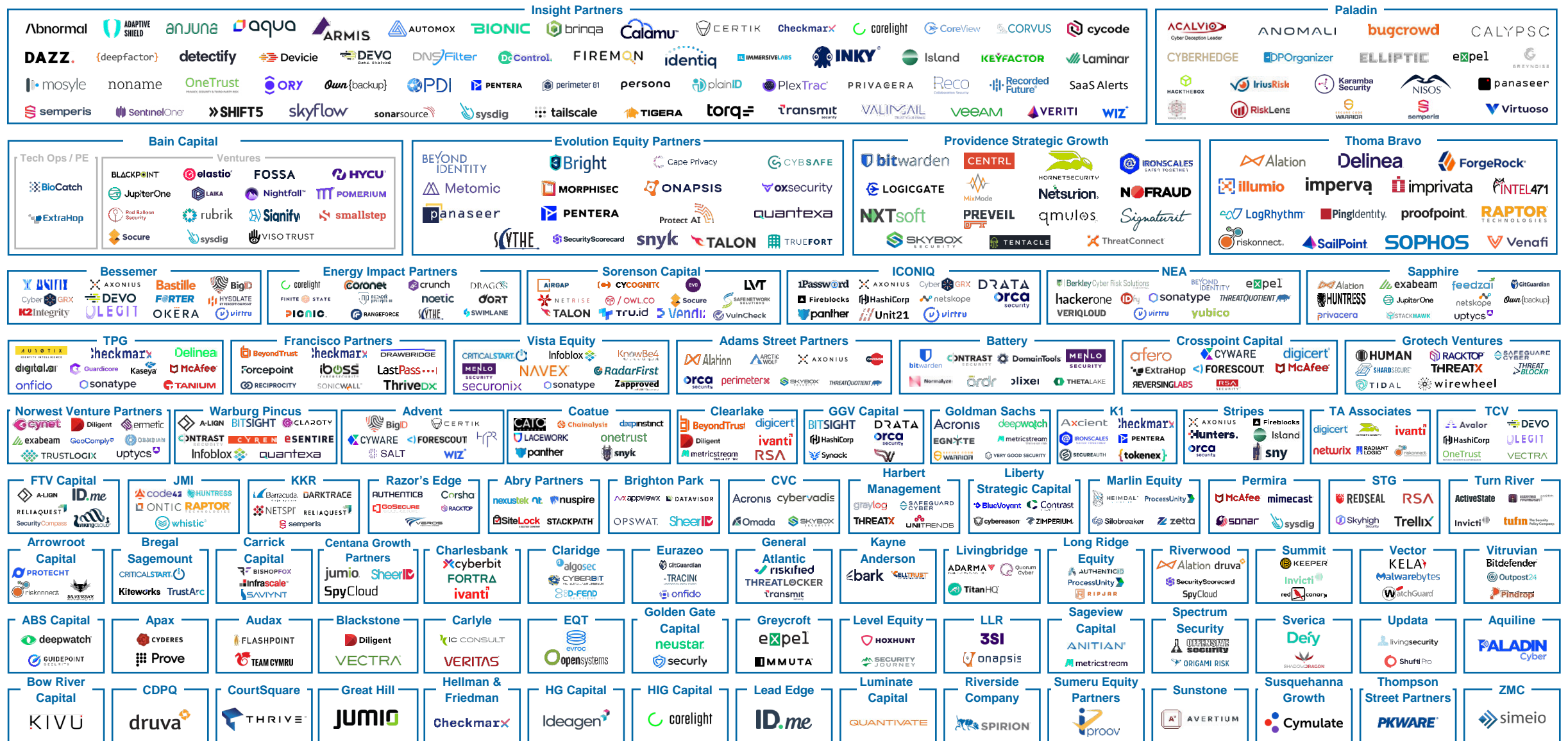
Selected Minority Transactions

(\$ in Millions)

Ann. Date	Lead Investor	Target	Amount	Valuation	Total Raised
Sep-19	Lightspeed	CATO NETWORKS	\$238	\$3,000	\$770
Sep-19	M12 MICROSOFT'S VENTURE FUND	HIDDENLAYER	\$50	NA	\$56
Sep-18	BlackRock KOCH DISRUPTIVE TECHNOLOGIES	DRAGO	\$274	\$1,974	\$432
Sep-05	Portage	THETARAY	\$57	NA	\$154
Sep-05	greylock	Upwind	\$50	\$300	\$77
Aug-16	RIVERWOOD CAPITAL	SpyCloud	\$110	\$410	\$169
Aug-07	[intact] VENTURES	resilience	\$100	\$950	\$221
Aug-03	Lightspeed	ENDOR LABS	\$48	\$115	\$70
Jul-31	CRAFT	HORIZON3.ai SECURE CODE WARRIOR	\$40	\$308	\$84
Jul-24	generation	onetrust	\$150	\$4,500	\$1,120
Jul-13	PALADIN CAPITAL GROUP	SECURE CODE WARRIOR	\$50	NA	\$165
Jul-10	evo/ution EQUITY PARTNERS	Protect AI	\$35	\$110	\$49

Sources: PitchBook, 451 Research as of September 30, 2023.
Notes: Valuation reflects estimated post-money valuation. NA indicates not available.

FINANCIAL SPONSORscape: Cybersecurity Portfolio Companies





Conferences and Events



Houlihan Lokey



Recent Conferences and Events

Conference Highlights



600+

Conference Attendees



70+

Participating Companies



Targeted

One-on-One Meetings With High-Profile Capital Providers

Upcoming Conferences and Events

Cybersecurity Focus: Panel Discussions and 1x1 Meetings

GenAI: The Next Frontier in Cybersecurity



Chris Inglis

Former U.S. National Cyber Director

HAKLUYT



D.J. Sampath

VP of Products, AI Cisco Secure



Brendan Hannigan

Co-Founder and CEO



J.Paul Haynes

President and COO

ESENTIRE

Participating Cybersecurity Companies



ESENTIRE

HYPR



Selected Conference Attendees



Apax

APOLLO



CARLYLE



GTCR

INSIGHT PARTNERS

KKR

MADISON DEARBORN PARTNERS



TCV

THOMABRAVO

VISTA

WARBURG PINCUS

3

October
2023

New York City | Lotte New York Palace



Recent Conferences and Events

WHAT TO EXPECT AT THE EVENT

- **Panel Discussions From CEOs at High-Growth Companies:** A wide range of speakers will share their insights about navigating current market conditions and positioning their companies for future success across a variety of technology sectors.
- **Featured Speakers:** The conference will feature high-profile speakers and candid panel discussions with distinguished tech thought leaders, discussing a variety of topical themes.
- **Targeted One-on-One Meetings:** Houlihan Lokey will arrange targeted, one-on-one meetings for presenting companies over the course of the conference, advising on prospects, meeting structure, and materials and coordinating any follow-up.
- **Networking Opportunities:** Join an audience of strategic, financial, and institutional investors as well as other capital providers for lunch and end-of-day cocktails.

14 March
2024

London | London Hilton on Park Lane

Upcoming Conferences and Events

AGENDA

MARCH 13

Evening Pre-Conference VIP Reception

MARCH 14

CONFERENCE:
Panels and 1x1s



Interested in presenting your company at GTC 2024 in London?

Email GTConference@HL.com

Recent Conferences and Events

- Black Hat is an internationally recognized cybersecurity event series providing the most technical and relevant security research.
- These multi-day events provide the security community with the latest cutting-edge research, developments, and trends.
- Attendees can gain hands-on experience and deepen their knowledge through a variety of training opportunities, including beginner- and advanced-level courses.

Black Hat USA 2023



The event includes four days of training and a two-day main conference featuring more than 100 selected Briefings, dozens of open-source tool demos in Black Hat Arsenal, Dark Reading, and more.



Black Hat CISO Summit is an approval-only event that brings together top security executives from global corporations and government agencies for a full day of unique discussions.



Key topics in the conference include AI and ML, AppSec, cloud security, cryptography, human factors, malware, mobile security, network security, policy, and privacy.

SUSTAINING PARTNERS



Upcoming Conferences and Events



Core Black Hat 2023 Features



Black Hat Briefings

Provides security professionals with a place to learn the very latest in information security risks, research, and trends.



Black Hat Trainings

Offers individual technical courses with topics ranging from the latest in penetration testing to exploiting web applications and defending and building SCADA systems.



Black Hat Certified Pentester

In partnership with The SecOps Group, Black Hat now has its own certification: Black Hat Certified Pentester.



Black Hat Business Hall

Solution providers and startups showcase the latest technologies and security services.

Recent Conferences and Events

- AWS re:Invent is a learning conference hosted by AWS for the global cloud computing community offering technical training sessions, workshops, and opportunities to connect with peers and experts.
- The conference features keynote announcements, training and certification opportunities, access to 2,000+ technical sessions, and numerous after-hours events.

AWS re:Invent



Innovation Talks: Deep dive into cloud computing topics with AWS subject-matter experts across analytics, databases, developer experience, and much more.



Keynotes: Hear from AWS leaders about what's top of mind for them, from innovations in infrastructure and AI/ML to the latest trends and breakthroughs in cloud computing.



Peer Talk Platform: Find, connect, and network with other attendees who share similar interests.

SELECTED SPONSORS



Upcoming Conferences and Events



Selected Cybersecurity Sessions

Move Fast, Stay Secure: Strategies for the Future of Security

Discover the AWS vision for security that drives business agility. Hear directly from security leaders as they share their insights on key topics like Zero Trust, builder security experience, and GenAI.



Chris Betz
CISO



Stephen Schmidt
VP, Security Engineer,
and CSO

AWS Security Best Practices

Eight-hour, deep-dive boot camp helps you learn to design and implement solutions to keep your workloads safe and secure. An expert AWS instructor dives deep into configuration best practices for specific tools to secure network infrastructure, harden compute resources, and quicken response to suspicious events.



Geraldine Lee
Global Delivery Readiness
Technical Lead

Data Protection and Resilience With AWS Storage

Dive deep into how AWS storage offers organizations defense-in-depth data protection and resilience across recovery point and time objectives, helping to mitigate risks around their application data at rest and in transit through policy-based access controls, encryption, and audit and reporting.



Palak Desai-Jambusaria
Head of Product



Bisman Sethi
Senior Technical PM

Bootcamps

Chalk Talks

Code Talks

Dev Chats

Workshops

Recent Conferences and Events

Upcoming Conferences and Events



- RSA Conference (RSAC) is the premier series of global events and year-round learning for the cybersecurity community.
- RSAC is the ultimate marketplace for the latest technologies and hands-on educational opportunities that help industry professionals discover how to make their companies more secure while showcasing the most enterprising, influential, and thought-provoking thinkers and leaders in cybersecurity today.
- The 2024 conference is centered around the theme “The Art of Possible,” underscoring the notion that cybersecurity professionals are akin to artists who rely on their intuition and collaborative efforts to craft solutions that unite us all in the pursuit of a more secure world.

Innovation Programs

Selected Sponsors



Innovation Sandbox

Cybersecurity’s boldest new innovators compete to put the spotlight on their game-changing ideas.



Launch Pad

Early-stage startups can pitch their new ideas *Shark Tank*-style to industry veterans for advice.



Sandbox

Offers immersive experiences featuring several interactive villages, the RSAC Cybrew Café, and cutting-edge research talks.



Early-Stage Expo

Exhibit space to discover and connect with 50+ rising stars in cybersecurity innovation.



Security Scholar

Hand-selected cybersecurity students are able to connect with the RSAC community.



Inclusive Security

Discuss how focus on inclusion has helped organizations improve their security postures.



AT&T Cybersecurity



COHESITY



KnowBe4



proofpoint.



The background features a hand holding a globe, with a network of lines and dots overlaid on the globe. The entire scene is set against a dark blue background with faint, glowing patterns.

IV

About Houlihan Lokey



Houlihan Lokey

Leading Independent, Global Advisory Firm



Houlihan Lokey is the trusted advisor to more top decision-makers than any other independent global investment bank.

2,686 Global Employees ⁽¹⁾	36 Locations ⁽¹⁾	\$7+ Billion Market Cap ⁽¹⁾	HLI LISTED NYSE	\$1.8 Billion Revenue ⁽²⁾	~25% Employee-Owned	No Debt
--	--------------------------------	---	------------------------------	---	------------------------	------------

Corporate Finance

- No. 1 Global M&A Advisor Under \$1 Billion
- Leading Capital Markets Advisor Raising Approximately \$25 Billion in Past Two Years

Rank	Advisor	Deals
1	Houlihan Lokey	381
2	Rothschild	369
3	JP Morgan	217

Source: Refinitiv.
Excludes accounting firms and brokers.

Financial Restructuring

- No. 1 Global Restructuring Advisor
- \$3.0+ Trillion of Aggregate Transaction Value Completed

Rank	Advisor	Deals
1	Houlihan Lokey	58
2	PJT Partners	30
3	Lazard	29

Source: Refinitiv.

Financial and Valuation Advisory

- No. 1 Global M&A Fairness Opinion Advisor Over the Past 25 Years
- 1,000+ Annual Valuation Engagements

Rank	Advisor	Deals
1	Houlihan Lokey	1,232
2	JP Morgan	1,030
3	Duff & Phelps, A Kroll Business	938

Source: Refinitiv.
Announced or completed transactions.

Financial Sponsors Coverage

- No. 1 Global Private Equity M&A Advisor
- 1,000+ Sponsors Covered Globally

Rank	Advisor	Deals
1	Houlihan Lokey	242
2	Lincoln International	192
3	Deloitte	190

Source: PitchBook.

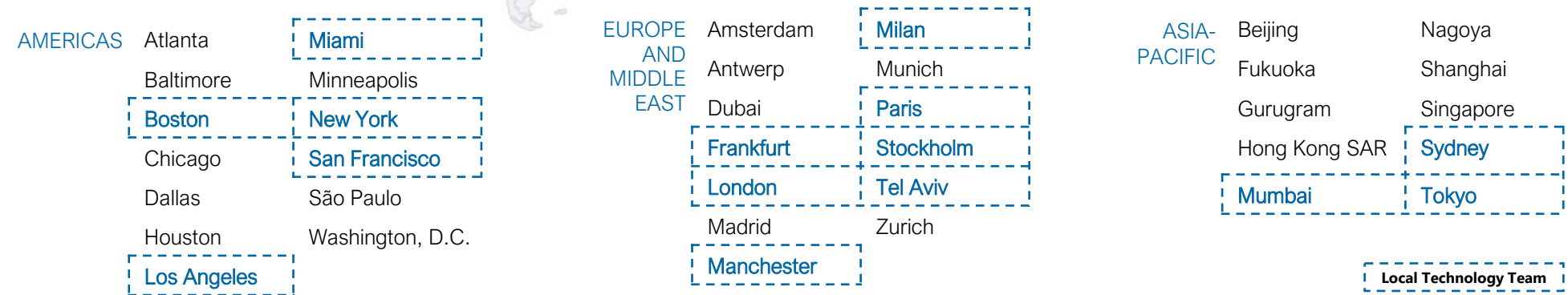
Houlihan Lokey has agreed to acquire 7 Mile Advisors, an independent advisory firm that provides a range of services to clients across the IT services sector.

The transaction, signed on July 7, will further enhance Houlihan Lokey's deep industry expertise in IT services and expand the firm's geographic footprint.

HQ: Charlotte, NC Employees: ~30 Managing Directors: 5

(1) As of October 30, 2023.
(2) LTM ended September 30, 2023.

Our Tech M&A Team Is No. 1 Globally With Unparalleled Reach



2022 M&A Advisory Rankings All Global Technology Transactions

Rank	Advisor	Deals
1	Houlihan Lokey	116
2	Goldman Sachs	106
3	Morgan Stanley	79
4	Rothschild	76
5	JP Morgan	75

Source: Refinitiv. Excludes accounting firms and brokers.



























































2022 M&A Advisory Rankings U.S. Technology Transactions Under \$1 Billion

Rank	Advisor	Deals
1	Houlihan Lokey	49
2	Canaccord Genuity Grp	37
2	Lincoln International	37
4	William Blair	33
5	Moelis	32

Source: Refinitiv. Excludes accounting firms and brokers.

*According to data provided by Refinitiv. Excludes accounting firms and brokers.

Deep Cybersecurity Experience Across the Ecosystem

 <p>has been acquired by</p>  <p>Sellside Advisor</p>	 <p>has been acquired by</p>  <p>Sellside Advisor</p>	<p>Transaction Pending</p>  <p>has agreed to acquire a majority stake in</p>  <p>formerly known as PROPHECY</p> <p>a portfolio company of</p>  <p>Buyside Advisor</p>	 <p>has received investment from</p>  <p>Sellside Advisor</p>	 <p>a portfolio company of</p>  <p>HoldCo PIK Notes Acquisition Financing</p> <p>Exclusive Placement Agent</p>	 <p>has been acquired by</p>  <p>Sellside Advisor</p>	 <p>has received a growth equity investment of \$70,000,000 from</p>  <p>Financial Advisor</p>
 <p>has made a strategic investment in</p>  <p>Buyside Advisor</p>	 <p>has received a strategic growth investment from</p>  <p>Sellside Advisor*</p>	 <p>has acquired a majority stake in</p>  <p>Your True Identity Company</p> <p>Buyside Advisor*</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>	 <p>has invested in</p>  <p>Financing Advisor*</p>	 <p>has sold a majority stake to</p>  <p>Sellside Advisor*</p>	 <p>has received an equity investment from</p>  <p>Financial Advisor</p>
 <p>has entered into a partnership with</p>  <p>Sellside Advisor*</p>	 <p>has invested in</p>  <p>Buyside Advisor*</p>	 <p>has sold a minority stake to</p>  <p>Sellside Advisor*</p>	 <p>structured equity investment led by</p>  <p>Financing Advisor*</p>	 <p>has been acquired by</p>  <p>Sellside Advisor</p>	 <p>has sold a majority stake in</p>  <p>to</p>  <p>Sellside Advisor*</p>	 <p>has acquired</p>  <p>Buyside Advisor</p>
<p>Acquisition Financing</p>  <p>has acquired</p>  <p>Financing Advisor*</p>	 <p>has sold substantially all its assets, pursuant to Section 363 of the U.S. Bankruptcy Code, to</p>  <p>Company Advisor</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>	 <p>has been acquired by</p>  <p>Sellside Advisor</p>	 <p>a portfolio company of</p>  <p>Financial Advisor</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>

Tombstones included herein represent transactions closed from 2010 forward.

*Selected transactions were executed by Houlihan Lokey professionals while at other firms acquired by Houlihan Lokey or by professionals from a Houlihan Lokey joint venture company.

How Houlihan Lokey Can Help


Our firm is extremely well-equipped to help our clients navigate uncertain times. We respond quickly to challenging situations and are constantly helping clients to analyze, structure, negotiate, and execute the best possible solutions from both a strategic and a financial perspective.

What We Offer

1  Corporate Finance


- Mergers and Acquisitions
- Capital Markets
- Private Funds Advisory
- Board Advisory Services

We are widely recognized as a leading M&A advisor to the mid-cap and have long-standing relationships with capital providers, including commercial banks and other senior credit providers, insurance funds, asset managers, and mezzanine fund investors. Few other investment banks maintain the breadth of relationships and capital markets intelligence that we do.

2  Financial Restructuring

- Company Advisory
- Special Situations
- Distressed M&A
- Liability Management
- Creditor Advisory

We have the largest restructuring practice of any global investment bank. Since 1988, we have advised on more than 1,500 restructuring transactions (with aggregate debt claims in excess of \$3.0 trillion). We served as an advisor in 12 of the 15 largest bankruptcies from 2000 to 2022.

3  Financial and Valuation Advisory

- Portfolio Valuation and Fund Advisory
- Transaction Opinions
- Corporate Valuation Advisory Services
- Transaction Advisory Services
- Real Estate Valuation and Advisory
- Dispute Resolution Consulting

Over five decades, we have established ourselves as one of the largest financial and valuation advisory firms. Our transaction expertise and leadership in the field of valuation help inspire confidence in the financial executives, boards of directors, special committees, investors, and business owners we serve.

Why We're Different



No. 1 for Global and U.S. Under \$1B Tech M&A*



Significant Experience With Financing Markets



Senior-Level Commitment and Dedication



Deep, Industry-Specific Expertise



Superior Work Product/Technical Abilities



Creativity, Imagination, Tenacity, and Positivity

*Source: Refinitiv. Excludes accounting firms and brokers.

Other Houlihan Lokey Cyber Sector Reports

GenAI in Cybersecurity Report



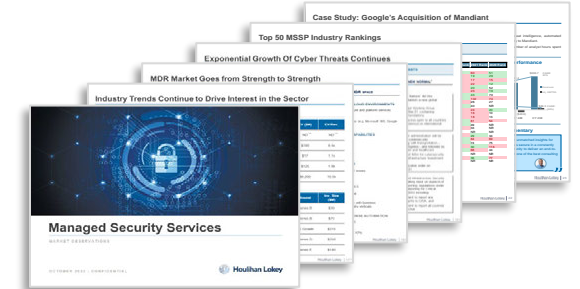
European Cybersecurity Idea Book



Identity Sector Report



Managed Security Services Report



To gain access to these decks, please reach out to the following:

U.S. Cyber Team



Keith Skirbe
Managing Director
Co-Head of U.S. Cyber
San Francisco
Keith.Skirbe@HL.com



Bobby Wolfe
Director
Co-Head of U.S. Cyber
Miami
BWolfe@HL.com



Joseph Miller
Associate
San Francisco
JJMiller@HL.com



Rishabh Bansal
Associate
San Francisco
Rishabh.Bansal@HL.com

Global Cyber Reach



Mark Smith
Director
Head of U.K. Cyber
Manchester
Mark.Smith@HL.com



Malte Abrams
Director
Head of DACH Cyber
Frankfurt
Malte.Abrams@HL.com



Ido Zakai
Managing Director
Head of Tech, Israel
Tel Aviv
Ido.Zakai@HL.com



Sara Napolitano
Managing Director
Head of France Cyber
Paris
Sara.Napolitano@HL.com

Capital Markets



Sean Fitzgerald
Managing Director
New York
SFitzgerald@HL.com



Chris Hebble
Managing Director
Los Angeles
CHebble@HL.com

Cyber Tech Expertise



Stephen Lee
Managing Director
Tech and Cyber Due Diligence
Chicago
SJLee@HL.com



Edouard Viot
Cybersecurity Consultant
Paris

Yearly Conferences





V




Appendix



Houlihan Lokey

High-Growth Cybersecurity Trading Metrics














(\$ in Millions, Except Price per Share)

Company	Stock Price	52-wk High	% of 52-wk High	YTD Stock Performance	Cash and ST Inv.	Equity Mkt Cap	Enterprise Value	EV/Revenue			EV/EBITDA		
								CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E
 CROWDSTRIKE	\$167.38	\$181.84	92.0%	62.1%	\$3,167	\$39,500	\$37,624	16.8x	12.4x	9.6x	NM	NM	39.3x
 zscaler	155.59	185.99	83.7%	41.2%	2,100	22,552	22,016	16.3x	11.9x	9.5x	NM	NM	46.1x
 SentinelOne	16.86	28.59	59.0%	15.7%	732	4,830	4,279	10.1x	7.1x	5.4x	NM	NM	NM

Top Quartile	\$31,026	\$29,820	16.6x	12.2x	9.6x	NM	NM	44.4x
Mean	\$22,294	\$21,306	14.4x	10.5x	8.2x	NM	NM	42.7x
Median	\$22,552	\$22,016	16.3x	11.9x	9.5x	NM	NM	42.7x
First Quartile	\$13,691	\$13,147	13.2x	9.5x	7.4x	NM	NM	41.0x

Medium-Growth Cybersecurity Trading Metrics

(\$ in Millions, Except Price per Share)







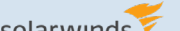





Company	Stock Price	52-wk High	% of 52-wk High	YTD Stock Performance	Cash and ST Inv.	Equity Mkt Cap	Enterprise Value	EV/Revenue			EV/EBITDA		
								CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E
 paloalto	\$234.44	\$258.88	90.6%	69.3%	\$2,390	\$80,249	\$72,288	11.7x	9.7x	8.1x	NM	32.1x	27.3x
 FORTINET.	58.68	81.24	72.2%	20.9%	3,314	46,648	43,834	9.9x	8.1x	6.9x	41.0x	28.6x	23.8x
 Gen	17.68	23.92	73.9%	(18.2%)	623	11,205	20,293	6.5x	5.3x	5.1x	14.0x	9.1x	9.3x
 okta	81.51	91.50	89.1%	17.2%	2,106	13,101	12,839	6.9x	5.8x	5.0x	NM	NM	43.0x
 CYBERARK	163.77	174.94	93.6%	29.7%	905	6,731	6,069	10.3x	8.3x	6.7x	NM	NM	NM
 Qualys.	152.55	157.88	96.6%	36.8%	349	5,827	5,247	10.7x	9.5x	8.5x	31.8x	21.3x	19.9x
 tenable	44.80	49.77	90.0%	18.2%	646	5,081	4,955	7.3x	6.3x	5.4x	NM	45.2x	36.5x
 RAPID7	45.78	55.61	82.3%	30.9%	294	2,731	3,412	5.0x	4.4x	3.9x	NM	30.4x	21.8x
 DARKTRACE	4.92	5.22	94.2%	54.5%	359	3,337	2,851	5.9x	4.7x	3.9x	NM	21.6x	21.3x
 BlackBerry	4.75	5.78	82.2%	43.0%	456	2,765	2,779	4.0x	3.4x	3.7x	NM	NM	NM
 F-Secure.	1.85	3.64	50.8%	(37.8%)	13	314	529	4.5x	3.9x	3.3x	12.8x	12.6x	9.2x
 Nitek	10.72	13.98	76.7%	10.4%	128	494	517	3.4x	3.0x	2.7x	11.7x	12.2x	8.5x
 riskified	4.48	6.73	66.6%	(2.8%)	474	771	350	1.3x	1.2x	1.0x	NM	NM	NM

Top Quartile	\$11,205	\$12,839	9.9x	8.1x	6.7x	31.8x	30.4x	26.4x
Mean	\$13,789	\$13,536	6.7x	5.7x	4.9x	22.2x	23.8x	22.0x
Median	\$5,081	\$4,955	6.5x	5.3x	5.0x	14.0x	21.6x	21.5x
First Quartile	\$2,731	\$2,779	4.5x	3.9x	3.7x	12.8x	13.0x	12.0x

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of September 30, 2023. Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Sorted by enterprise value. Growth categorizations are based on 2022A–2023E revenue growth breakpoints; high-growth ≥ 30%, medium-growth >10% and <30%, low-growth ≤ 10%.

Low-Growth Cybersecurity Trading Metrics




(\$ in Millions, Except Price per Share)

Company	Stock Price	52-wk High	% of 52-wk High	YTD Stock Performance	Cash and ST Inv.	Equity Mkt Cap	Enterprise Value	EV/Revenue			EV/EBITDA		
								CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E
 BROADCOM	\$830.58	\$923.67	89.9%	50.1%	\$12,055	\$346,352	\$370,096	10.8x	10.2x	9.4x	18.5x	15.7x	15.5x
 splunk >	146.25	147.14	99.4%	68.5%	2,449	24,089	26,269	7.2x	6.7x	6.0x	NM	27.6x	23.8x
 opentext	35.10	43.25	81.2%	16.7%	1,234	9,494	17,409	2.8x	3.1x	2.9x	9.3x	7.8x	6.6x
 CHECK POINT	133.28	138.60	96.2%	5.1%	1,457	15,929	12,098	5.2x	5.0x	4.8x	13.3x	11.3x	10.9x
 TREND MICRO	161.14	167.89	96.0%	11.2%	803	9,712	9,158	3.4x	3.3x	3.2x	18.2x	9.1x	NA
 SolarWinds	37.95	52.96	71.7%	(19.2%)	1,808	5,281	3,372	2.0x	2.0x	1.9x	7.9x	9.0x	8.5x
 Securworks	9.44	12.22	77.3%	0.2%	178	1,534	2,648	3.7x	3.6x	3.4x	13.8x	8.5x	8.0x
 OneSpan	6.21	10.06	61.7%	(1.1%)	65	529	480	1.0x	1.3x	1.3x	NM	NM	35.8x
 Cognyte	10.75	19.25	55.8%	(7.3%)	83	435	354	1.6x	1.6x	1.5x	NM	NM	7.5x
 W / T H secure	4.81	6.23	77.2%	50.8%	72	349	291	0.9x	0.9x	0.9x	NM	NM	NM
 Telos	1.09	1.84	59.2%	(25.5%)	38	187	154	1.1x	1.0x	0.9x	NM	NM	NM
 Telos	2.39	11.24	21.3%	(53.9%)	103	163	75	0.3x	0.6x	0.5x	NM	NM	NM
Top Quartile						\$11,266	\$13,426	4.1x	3.9x	3.7x	17.1x	13.5x	17.6x
Mean						\$34,504	\$36,867	3.3x	3.3x	3.1x	13.5x	12.7x	14.6x
Median						\$3,407	\$3,010	2.4x	2.6x	2.4x	13.5x	9.1x	9.7x
First Quartile						\$413	\$338	1.1x	1.2x	1.2x	10.3x	8.7x	7.9x

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of September 30, 2023. Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Sorted by enterprise value. Growth categorizations are based on 2022A–2023E revenue growth breakpoints; high-growth ≥ 30%, medium-growth >10% and <30%, low-growth ≤ 10%.

High-Growth Cybersecurity Operating Metrics

(\$ in Millions, Except Price per Share)

Company	Stock Price	Equity Mkt Cap	Enterprise Value	Revenue			EBITDA			Revenue Growth			EBITDA Margin		
				CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E	2021–2022A	2022A–2023E	2023–2024E	CY 2022A	CY 2023E	CY 2024E
 CROWDSTRIKE	\$167.38	\$39,500	\$37,624	\$2,241	\$3,039	\$3,906	(\$118)	\$729	\$956	54.4%	35.6%	28.5%	NM	24.0%	24.5%
 zscaler	155.59	22,552	22,016	1,348	1,844	2,310	(272)	361	477	56.8%	36.8%	25.3%	NM	19.6%	20.7%
 SentinelOne	16.86	4,830	4,279	422	606	799	(374)	(145)	(10)	106.1%	43.5%	31.8%	NM	NM	NM

Top Quartile	\$31,026	\$29,820	\$1,795	\$2,441	\$3,108	(\$195)	\$545	\$717	81.5%	40.1%	30.2%	NM	22.9%	23.5%
Mean	\$22,294	\$21,306	\$1,337	\$1,830	\$2,338	(\$255)	\$315	\$474	72.5%	38.6%	28.6%	NM	21.8%	22.6%
Median	\$22,552	\$22,016	\$1,348	\$1,844	\$2,310	(\$272)	\$361	\$477	56.8%	36.8%	28.5%	NM	21.8%	22.6%
First Quartile	\$13,691	\$13,147	\$885	\$1,225	\$1,554	(\$323)	\$108	\$234	55.6%	36.2%	26.9%	NM	20.7%	21.6%

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of September 30, 2023. Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Sorted by enterprise value. Growth categorizations are based on 2022A–2023E revenue growth breakpoints; high-growth ≥ 30%, medium-growth >10% and <30%, low-growth ≤ 10%.

Medium-Growth Cybersecurity Operating Metrics

(\$ in Millions, Except Price per Share)





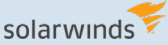




Company	Stock Price	Equity Mkt Cap	Enterprise Value	Revenue			EBITDA			Revenue Growth			EBITDA Margin		
				CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E	2021–2022A	2022A–2023E	2023–2024E	CY 2022A	CY 2023E	CY 2024E
paloalto	\$234.44	\$80,249	\$72,288	\$6,156	\$7,487	\$8,917	\$245	\$2,249	\$2,652	26.7%	21.6%	19.1%	4.0%	30.0%	29.7%
FORTINET	58.68	46,648	43,834	4,417	5,405	6,374	1,069	1,533	1,846	32.2%	22.4%	17.9%	24.2%	28.4%	29.0%
Gen	17.68	11,205	20,293	3,107	3,812	3,945	1,454	2,220	2,178	12.9%	22.7%	3.5%	46.8%	58.2%	55.2%
okta	81.51	13,101	12,839	1,858	2,216	2,578	(662)	228	299	37.7%	19.3%	16.3%	NM	10.3%	11.6%
CYBERARK	163.77	6,731	6,069	592	731	908	(136)	23	81	17.7%	23.6%	24.2%	NM	3.2%	8.9%
Qualys	152.55	5,827	5,247	490	554	621	165	247	264	19.1%	13.2%	12.0%	33.7%	44.5%	42.5%
tenable	44.80	5,081	4,955	683	789	910	(43)	110	136	26.3%	15.5%	15.4%	NM	13.9%	14.9%
RAPID7	45.78	2,731	3,412	685	774	873	(70)	112	157	28.0%	12.9%	12.9%	NM	14.5%	17.9%
DARKTRACE	4.92	3,337	2,851	484	602	740	35	132	134	38.5%	24.4%	22.9%	7.2%	21.9%	18.1%
BlackBerry	4.75	2,765	2,779	690	826	746	(91)	2	34	(7.1%)	19.8%	(9.8%)	NM	0.2%	4.5%
F-Secure	1.85	314	529	119	137	158	41	42	57	(1.8%)	15.6%	15.5%	34.8%	30.5%	36.2%
Mittek	10.72	494	517	150	170	191	44	40	61	18.9%	13.2%	12.5%	29.5%	23.3%	31.9%
riskified	4.48	771	350	261	301	353	(105)	(16)	6	14.0%	15.3%	17.4%	NM	NM	1.6%

Top Quartile	\$11,205	\$12,839	\$1,858	\$2,216	\$2,578	\$165	\$247	\$299	28.0%	22.4%	17.9%	34.3%	30.2%	31.9%
Mean	\$13,789	\$13,536	\$1,515	\$1,831	\$2,101	\$150	\$532	\$608	20.2%	18.4%	13.8%	25.7%	23.3%	23.2%
Median	\$5,081	\$4,955	\$683	\$774	\$873	\$35	\$112	\$136	19.1%	19.3%	15.5%	29.5%	22.6%	18.1%
First Quartile	\$2,731	\$2,779	\$484	\$554	\$621	(\$91)	\$40	\$61	14.0%	15.3%	12.5%	15.7%	13.0%	11.6%

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of September 30, 2023. Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Sorted by enterprise value. Growth categorizations are based on 2022A–2023E revenue growth breakpoints; high-growth ≥ 30%, medium-growth >10% and <30%, low-growth ≤ 10%.

Low-Growth Cybersecurity Operating Metrics

(\$ in Millions, Except Price per Share)

Company	Stock Price	Equity Mkt Cap	Enterprise Value	Revenue			EBITDA			Revenue Growth			EBITDA Margin		
				CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E	2021–2022A	2022A–2023E	2023–2024E	CY 2022A	CY 2023E	CY 2024E
 BROADCOM	\$830.58	\$346,352	\$370,096	\$34,412	\$36,330	\$39,267	\$20,005	\$23,530	\$23,920	20.7%	5.6%	8.1%	58.1%	64.8%	60.9%
splunk >	146.25	24,089	26,269	3,654	3,948	4,409	(126)	952	1,104	36.7%	8.0%	11.7%	NM	24.1%	25.0%
opentext	35.10	9,494	17,409	6,234	5,630	5,983	1,867	2,239	2,656	(0.4%)	(9.7%)	6.3%	30.0%	39.8%	44.4%
 CHECK POINT	133.28	15,929	12,098	2,330	2,414	2,519	909	1,071	1,105	7.5%	3.6%	4.4%	39.0%	44.4%	43.9%
	161.14	9,712	9,158	2,709	2,807	2,872	502	1,001	0	1.6%	3.6%	2.3%	18.5%	35.7%	NM
 TREND MICRO	37.95	5,281	3,372	1,697	1,651	1,766	429	376	397	2.6%	(2.7%)	7.0%	25.3%	22.8%	22.5%
 solarwinds	9.44	1,534	2,648	719	744	781	192	310	331	0.1%	3.5%	4.9%	26.7%	41.7%	42.4%
Secureworks	6.21	529	480	463	362	358	(111)	(34)	13	(13.4%)	(21.9%)	(1.2%)	NM	NM	3.8%
 OneSpan	10.75	435	354	219	227	236	(7)	2	47	2.1%	3.7%	3.8%	NM	0.7%	20.0%
 Cognyte	4.81	349	291	312	307	326	(90)	(7)	3	(34.2%)	(1.6%)	6.1%	NM	NM	1.0%
 W / T H secure	1.09	187	154	144	153	168	(44)	(22)	(2)	(2.6%)	6.5%	9.8%	NM	NM	NM
 Telos	2.39	163	75	217	130	137	(49)	(15)	(12)	(10.5%)	(39.9%)	5.4%	NM	NM	NM
Top Quartile		\$11,266	\$13,426	\$2,945	\$3,092	\$3,256	\$604	\$1,019	\$1,104	3.9%	4.2%	7.2%	36.7%	42.3%	43.9%
Mean		\$34,504	\$36,867	\$4,426	\$4,559	\$4,902	\$1,956	\$2,450	\$2,464	0.9%	(3.4%)	5.7%	32.9%	34.2%	29.3%
Median		\$3,407	\$3,010	\$1,208	\$1,198	\$1,273	\$93	\$343	\$189	0.9%	3.5%	5.8%	28.3%	37.7%	25.0%
First Quartile		\$413	\$338	\$289	\$287	\$303	(\$59)	(\$9)	\$2	(4.6%)	(4.5%)	4.2%	25.6%	23.8%	20.0%

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of September 30, 2023. Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Sorted by enterprise value. Growth categorizations are based on 2022A–2023E revenue growth breakpoints; high-growth ≥ 30%, medium-growth >10% and <30%, low-growth ≤ 10%.

Disclaimer

© 2023 Houlihan Lokey. All rights reserved. This material may not be reproduced in any format by any means or redistributed without the prior written consent of Houlihan Lokey.

Houlihan Lokey is a trade name for Houlihan Lokey, Inc., and its subsidiaries and affiliates, which include the following licensed (or, in the case of Singapore, exempt) entities: in (i) the United States: Houlihan Lokey Capital, Inc., and Houlihan Lokey Advisors, LLC, each an SEC-registered broker-dealer and member of FINRA (www.finra.org) and SIPC (www.sipc.org) (investment banking services); (ii) Europe: Houlihan Lokey Advisory Limited, Houlihan Lokey EMEA, LLP, Houlihan Lokey (Corporate Finance) Limited, and Houlihan Lokey UK Limited, authorized and regulated by the U.K. Financial Conduct Authority; Houlihan Lokey (Europe) GmbH, authorized and regulated by the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht); (iii) the United Arab Emirates, Dubai International Financial Centre (Dubai): Houlihan Lokey (MEA Financial Advisory) Limited, regulated by the Dubai Financial Services Authority for the provision of advising on financial products, arranging deals in investments, and arranging credit and advising on credit to professional clients only; (iv) Singapore: Houlihan Lokey (Singapore) Private Limited and Houlihan Lokey Advisers Singapore Private Limited, each an “exempt corporate finance adviser” able to provide exempt corporate finance advisory services to accredited investors only; (v) Hong Kong SAR: Houlihan Lokey (China) Limited, licensed in Hong Kong by the Securities and Futures Commission to conduct Type 1, 4, and 6 regulated activities to professional investors only; (vi) India: Houlihan Lokey Advisory (India) Private Limited, registered as an investment adviser with the Securities and Exchange Board of India (registration number INA000001217); and (vii) Australia: Houlihan Lokey (Australia) Pty Limited (ABN 74 601 825 227), a company incorporated in Australia and licensed by the [Australian Securities and Investments Commission](#) (AFSL number 474953) in respect of financial services provided to wholesale clients only. In the United Kingdom, European Economic Area (EEA), Dubai, Singapore, Hong Kong, India, and Australia, this communication is directed to intended recipients, including actual or potential professional clients (UK, EEA, and Dubai), accredited investors (Singapore), professional investors (Hong Kong), and wholesale clients (Australia), respectively. No entity affiliated with Houlihan Lokey, Inc., provides banking or securities brokerage services and is not subject to FINMA supervision in Switzerland or similar regulatory authorities in other jurisdictions. Other persons, such as retail clients, are NOT the intended recipients of our communications or services and should not act upon this communication.

Houlihan Lokey gathers its data from sources it considers reliable; however, it does not guarantee the accuracy or completeness of the information provided within this presentation. The material presented reflects information known to the authors at the time this presentation was written, and this information is subject to change. Any forward-looking information and statements contained herein are subject to various risks and uncertainties, many of which are difficult to predict, that could cause actual results and developments to differ materially from those expressed in, or implied or projected by, the forward-looking information and statements. In addition, past performance should not be taken as an indication or guarantee of future performance, and information contained herein may be subject to variation as a result of currency fluctuations. Houlihan Lokey makes no representations or warranties, expressed or implied, regarding the accuracy of this material. The views expressed in this material accurately reflect the personal views of the authors regarding the subject securities and issuers and do not necessarily coincide with those of Houlihan Lokey. Officers, directors, and partners in the Houlihan Lokey group of companies may have positions in the securities of the companies discussed. This presentation does not constitute advice or a recommendation, offer, or solicitation with respect to the securities of any company discussed herein, is not intended to provide information upon which to base an investment decision, and should not be construed as such. Houlihan Lokey or its affiliates may from time to time provide financial or related services to these companies. Like all Houlihan Lokey employees, the authors of this presentation receive compensation that is affected by overall firm profitability.



Houlihan Lokey



CORPORATE FINANCE
FINANCIAL RESTRUCTURING
FINANCIAL AND VALUATION ADVISORY

HL.com