INTRODUCTION

We are pleased to present our 2019 second quarter Cybersecurity Capital Markets, Mergers & Acquisitions (M&A) Update which highlights key trends and statistics for the second quarter.

Increasingly sophisticated cyber attacks, coupled with the widespread adoption of cloud computing and internet of things (IoT) technology, has fueled demand for effective cybersecurity solutions. As cyber crime damages continue to reach heightened levels, industry operators have allocated increased resources towards cybersecurity budgets, with global spending forecasted to exceed $1 trillion by 2021, according to Cyber Security Ventures. \(^1\) As cyber criminals and nation-state actors continue to penetrate information technology (IT) networks and sensitive infrastructure, companies offering innovative and effective solutions are poised to capture further market share and higher valuations.

Transaction activity in the Cybersecurity industry has continued to reflect solid growth with 61 closed transactions in Q2 2019, a moderate increase from the previous quarter. Through Q2 2019 total disclosed deal value has exceeded $22 billion, compared to approximately $15.8 billion through Q2 2018.

This report provides key insights into the cybersecurity transaction environment, focusing on the following:

- Q2 2019 M&A Activity & Venture Capital Investments
- Q2 2019 Public Company Performance

In addition for this quarter we have included information on the following:

- Manufacturing Cybersecurity
- Managed Security Service Providers
- Managed Security Service Market Outlook
- Data Protection Market Outlook

To learn more about Capstone Headwaters’ Cybersecurity practice or to discuss the content of this report, please contact Tom McConnell or David Brinkley.
M&A OVERVIEW

M&A activity in Q2 2019 in the Cybersecurity industry remained robust with 61 completed transactions, slightly below historic highs. Total transaction value reached nearly $9.9 billion as consolidation continues to be fueled by the demand for innovative and cost-effective cybersecurity solutions.

NOTABLE TRANSACTIONS

- Orange S.A has acquired SecureLink N.V. (June) for $576 million equating to a 2.1x TTM (Trailing Twelve Months) revenue multiple. Orange will leverage SecureLink’s consulting, managed incident detection and response, and security maintenance capabilities to accelerate its expansion into European markets.

- Elastic N.V (NYSE:ESTC) has acquired Endgame, Inc. (June) for $234 million, equivalent to 11.8x LTM revenue. The acquisition advances Elastic’s endpoint security solutions and will integrate Endgame’s offerings into its security information and event management platform (SIEM).

- Avast Plc (LSE:AVST) acquired Baltimore-based TrackOFF, Inc. (May) for an undisclosed sum, enhancing its data privacy capabilities.

- Insight Partners has acquired leading threat intelligence provider, Recorded Future, for an enterprise value of $780 million. Recorded Future will leverage Insight’s sector expertise and internal consulting arm, Insight Onsite, to achieve further growth and scale.

- FireEye (Nasdaq:FEYE) has acquired Verodin (May) for approximately $250 million. Verodin’s platform will be integrated into FireEye’s security orchestration capabilities to enhance its identification of gaps in security effectiveness.

- NuMSP has acquired managed IT services provider (MSP), NetFusion, Inc. (May), for an undisclosed sum. The transaction expands NuMSP’s footprint into the Los Angeles market and marks its 13th acquisition since August 2018.
PUBLIC COMPANY PERFORMANCE

Public cybersecurity company valuations remained steady through Q2 2019, with HACK ETF EBITDA and Revenue multiples reaching 25.2x and 3.5x, respectively. Notable public players such as Palo Alto (NYSE:PANW), Cisco Systems (Nasdaq:CSCO), Splunk (Nasdaq:SPLK), and CyberArk (Nasdaq:CYBR) posted strong revenue growth in their most recent earnings releases.

The overall U.S. initial public offering (IPO) market rebounded following a lackluster Q1 2019, with 66 companies filing for public listing raising a total of $27 billion, according to Ernst & Young.2 The Cybersecurity industry has contributed several recent significant IPOs in 2019 – CrowdStrike (Nasdaq:CRWD) in June raised $612 million in its IPO, valuing the company at $6.7 billion; Tufin (NYSE:TUFN) raised $124 million in April, valuing the company at approximately $563.6 million; and Ping Identity raised $187.5 million in its September IPO, valuing the company at $1.16 billion.

FINANCING ACTIVITY

Financing activity in Q2 2019 eclipsed record levels seen in Q1 2019 as financial sponsors have continued to deploy significant sums of capital towards the sector. Building on the momentum in Q1, nearly $2.3 billion of capital was raised across 108 fundraising deals in Q2 2019. Notable cybersecurity venture capital raises in Q2 2019 include:

- KnowBe4, Inc. raised $309.4 million in an investment led by KKR & Co. Inc. (NYSE:KKR) with participation from Elephant and TenEleven Ventures. The infusion of capital is expected to be utilized for global growth initiatives and values KnowBe4 at $1 billion post-investment.

- Vectra AI Inc., a leading provider of network threat detection and response (NDR), raised $100 million of Series E venture funding (June, post-valuation of $420 million) in a deal led by TCV. The financing will be used to accelerate global expansion and establish a market leading position for its Cognito cloud security platform.

- SentinelOne Inc., a cybersecurity provider specializing in autonomous endpoint protection, raised $120 million in a Series D fundraising round (May, post-valuation of $600 million) led by Insight Partners. The deal highlights the heightened demand for endpoint protection, an industry expected to exceed $13.1 billion by 2022, according to the Radicati Group.3

- Auth0, Inc., a premier identity management security provider, raised $103 million in a Series E funding round led by Sapphire Venture Partners. The transaction elevates Auth0’s valuation to $1.16 billion as it looks to expand its customer base and global reach.
COMPUTER SPOTLIGHT

**Pong Identity**

**Founded:** 2001  
**Ticker:** NYSE:PING  
**Headquartered:** Denver, CO  
**IPO Date:** 9/19/19  
**Current Price:** $16.51 (as of 10/08/19)

Denver-based Ping Identity (NYSE:PING) is a leading identity security provider that offers real-time intelligent access solutions to the Financial Services, Healthcare, Public Sector, Manufacturing, and Retail industries. Its proprietary Ping Intelligent Identity platform leverages artificial intelligence (AI) and machine learning to provide a diverse range of options to enhance digital business capabilities with multi-factor authentication, single sign-on, access management, intelligent API security, and data governance solutions. Ping Intelligent Identity is utilized by over half of all Fortune 100 companies including Boeing (NYSE:BA), Cisco (Nasdaq:CSCO), Disney (NYSE:DIS), GE (NYSE:GE), and Walgreens (Nasdaq:WBA). Among recent case studies, Thomson Reuters reported that it has saved $1.2 million by leveraging Ping’s platform to enhance its authentication infrastructure.4

Ping raised $187.5 million in its IPO on the New York Stock Exchange in September and sold 12,500,000 shares at $15 per share, valuing the company at $1.16 billion. In its trading debut, Ping’s stock price surged 34% in the midst of a season of mixed market results among notable IPOs. The PE-backed identity management provider was acquired by Vista Equity Partners in June 2016 for an enterprise value of $600 million. The acquisition came on the heels of monumental customer growth and business momentum as Ping’s annual recurring revenue had grown by more than 40% in 2015.5

**Case Study: NETFLIX**

Netflix (Nasdaq:NFLX) employed Ping to enhance its cloud identity solution which was affecting its employees’ ability to authenticate user identity. Ping implemented its PingFederate platform, leveraging three levels of adaptive authentication to ensure that the right user is gaining access. As a result of this tool, Netflix’s identity and access management team (IAM) experienced significantly less requests for client management, allowing additional focus on other identity solutions.

**Case Study: HEWLETT-PACKARD**

HP Inc. (NYSE:HPQ) employed Ping to assist with its fragmented user base that consisted of more than a dozen identity management and authentication systems. Ping created a common user interface flow for identity registration and login, utilizing single sign-on to enable a new centralized service. This allowed HP to leverage a single IAM platform deployed across the entire organization in order to drive efficiency and reduce complexity.

---

**Timeline:**

- **2011:** Ping raised $21 million of Series E funding in June 2016, putting its post-money valuation at $129.02 million.
- **2013:** Ping raised $44 million in a Series F funding round led by W Capital Partners and DFJ Growth. The company’s post-money valuation was $238.08 million.
- **2014:** Ping Raised $35 million in a Series G funding round led by KKR and TenEleven Ventures. The company’s post-money valuation was $286.76 million.
- **2016:** Vista Equity Partners acquired Ping on June 30th for an enterprise value of $600 million.
- **2019:** Ping raised $187.5 million in its IPO, valuing the company at $1.16 billion.
SEGMENT HIGHLIGHT: Industrial & Manufacturing

Industrial & Manufacturing operators have continued to digitize their IT and Operation Technology (OT) solutions, fostering demand for increasingly sophisticated industrial control systems (ICS). As IoT capabilities promote automation and interconnectivity, there is a heightened need for mitigation of cybersecurity risks. Over the previous twelve months, 50% of industrial executives reported a data breach or cyber attack, according to Sikich 2019 Manufacturing and Distribution Survey.5

There is a wide disparity in cybersecurity capabilities between large and small manufacturing operators. The lack of readily available cyber talent has presented challenges for operators, especially for small to medium-sized businesses (SMBs) who may not have the capital resources to allocate significant spending to retain IT human capital. Thirty-seven percent of companies with less than $500 million in revenue hire cyber talent to combat attacks, compared to 69% among those with greater than $500 million in revenue, according to Sikich.

### Top Cyber Threats among Manufacturers

<table>
<thead>
<tr>
<th>Threat</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Theft</td>
<td>34%</td>
</tr>
<tr>
<td>Phishing &amp; Pharming</td>
<td>32%</td>
</tr>
<tr>
<td>Threat Sophistication</td>
<td>28%</td>
</tr>
<tr>
<td>Third Party Breaches</td>
<td>28%</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>27%</td>
</tr>
<tr>
<td>Employee Error</td>
<td>26%</td>
</tr>
</tbody>
</table>

*Source: Deloitte*

### Actions Taken To Enhance Cybersecurity

<table>
<thead>
<tr>
<th>Action</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partnering with Outside Firm</td>
<td>42% ($&lt;500 mm in Revenue)</td>
</tr>
<tr>
<td>Cyber Audits</td>
<td>57% ($&lt;500 mm in Revenue)</td>
</tr>
<tr>
<td>Hiring Cybersecurity Talent</td>
<td>63% ($&lt;500 mm in Revenue)</td>
</tr>
<tr>
<td>Phishing Exercises</td>
<td>69% ($&lt;500 mm in Revenue)</td>
</tr>
</tbody>
</table>

*Source: Sikich 2019 Manufacturing & Distribution Survey*

### Transaction Activity

As manufacturers are exposed to a growing number of cyber breach points on account of connected devices, digital supply chains, and legacy control systems; cybersecurity providers that can offer cost-efficient solutions present valuable M&A opportunities. Recent transaction activity has demonstrated the demand for industrial cybersecurity providers that offer innovative applications to address mounting cyber concerns.

Ampcus Cyber acquired Orbit Cyber Inc. in September (undisclosed) to expand its global footprint and enhance its services delivery network. Orbit specializes in industrial OT and IT domains and offers comprehensive assessments of access, firewall, and OT security controls for assets connecting from the industrial systems to the cloud. In addition, Palo Alto Networks (NYSE:PANW) acquired leading industrial IoT security solutions provider, ZingBox Inc. for an enterprise value of $75 million (September). Zingbox’s IoT Command Center platform offers manufacturers an IoT lifecycle management solution that delivers security and optimization of connected devices in physical systems. It provides real-time vulnerability assessment and integration of IT and OT intelligence. In May, Sectigo acquired Icon Labs (undisclosed), a leading provider of cross-platform security solutions for embedded original equipment manufacturer and IoT device manufacturers. The acquisition enhances Sectigo’s IoT security platform to provide robust connected device security.

Intellectual property (IP) is among the most valuable assets for manufacturers and is also frequently targeted by hackers. IP theft was cited as the top cybersecurity threat among manufacturing executives (34%), according to Deloitte.7 IP theft is especially prevalent among operators that have a global presence, increasing exposure to cyber threats by other countries which has necessitated complex risk measures.
SEGMENT HIGHLIGHT: Managed Security Service Providers

$35B  GLOBAL MANAGED SECURITY SERVICES MARKET SIZE BY 2022

Increasing interoperability of IoT applications and connected devices have fueled demand for managed security service providers (MSSPs). With nearly 7.7 million IoT devices connected to the internet every day (NetScout) there are an abundance of network vectors for bad actors to penetrate. The prevalence of increasing cyber threats has contributed to the $35 billion forecasted MSSP market value by 2022, according to Cyber Defense Magazine.

MSSPs often offer a more cost-effective solution than building out in-house IT infrastructure support, especially for small to medium-sized businesses (SMBs). Providers of outsourced real-time threat prevention, network and firewall protection, and data encryptions can optimize operators’ digital business processes. MSSPs have fostered increasing demand among SMBs, as 29% of IT security operations were supported by MSSP in 2018, compared to 21% in 2017, according to Ponemon Institute.

Labor market dynamics in the Cybersecurity industry have also contributed towards MSSP growth, as the industry is expected to experience 3.5 million unfilled positions by 2021, according to The Herjavec Group. The shortage of available talent has caused many operators to employ MSSPs, especially among smaller operators that lack the resources to hire full-time IT expertise. Operators have increasingly allocated spending towards security awareness training to mitigate employee-induced breaches and cyber attacks. MSSPs will frequently provide security awareness training as a part of its suite of services, a market that is expected to reach $10 billion by 2027, according to Cybersecurity Ventures.

Transaction activity in the MSSP market has remained healthy through Q2 2019, both domestically and internationally. Notably, Capstone Headwaters advised leading managed detection and response (MDR) provider, Rook Security, on its acquisition by Sophos (LSE:SOPH). Terms of the deal were not disclosed. The acquisition integrates Rook Security’s MDR capabilities with Sophos’ expansive technology and product portfolio and enhances Sophos’ customer offerings. In May, Swisscom AG (SWX:SCMN) acquired United Security Providers AG (undisclosed), creating a market leading MSSP platform in the Swiss Cybersecurity industry. In addition, Coretelligent, LLC acquired leading managed IT services provider United Technology Group, LLC. United Technology will leverage Coretelligent’s national platform and technology resources to enhance its core competencies and customer network.

Active Buyer Profile: NuMSP

New Jersey-based NuMSP is a leading MSP offering IT and security service solutions for SMBs. Through Q2 2019, NuMSP has remained highly acquisitive as it looks to scale operations to provide a national security services platform, having acquired seven companies in 2019. Recent NuMSP transactions include:

<table>
<thead>
<tr>
<th>Target</th>
<th>Investment Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>NuMSP</td>
<td>Acquired full service MSP, J and J Technical Services, in June (deal value undisclosed) in order to increase penetration in the New Mexico market for comprehensive IT services.</td>
</tr>
<tr>
<td>NuMSP</td>
<td>Acquired full service MSP, AZBS, Inc. in April for an undisclosed sum. AZBS is a full service MSP offering IT solutions for SMBs. The transaction allows NuMSP to establish a greater presence in the Chicago MSP market.</td>
</tr>
</tbody>
</table>

In the recent past, NuMSP acquired NetFusion (May, undisclosed), an MSP specializing in information security, expands NuMSP’s reach into the Los Angeles Cyber markets.
MARKET OUTLOOKS

Managed Security Services Market Outlook

The global Managed Security Services market is projected to increase from $24 billion in 2018 to nearly $48 billion in 2023, according to Markets and Markets.\(^\text{13}\)

![Global Managed Cybersecurity Services Market](image)

Managed cybersecurity service providers can offer a variety of solutions, from managed identity and access management (IAM) to firewall management, providing a flexible and cost-efficient alternative to building out internal capabilities.

Global distributed denial-of-service (DDoS) attacks increased to 3.8 million in the first half of 2019, a 39% year-over-year increase, according to NetScout.

The IAM industry is expected to continue to experience robust growth, as global spending on products and services are forecasted to exceed $16 billion, according to Cybersecurity Ventures.\(^\text{14}\)

Data Protection Market Outlook

The United States possesses the highest average cost per data breach out of all nations at $8.19 million per breach, according to the Ponemon Institute.\(^\text{15}\) The need for sophisticated data protection solutions has fueled demand in this market which is expected to reach $125.8 billion by 2023, according to KBV Research.\(^\text{16}\)

![Data Protection Market](image)

The Healthcare industry has experienced the highest average total cost of a data breach at $6.45 million, 65% higher than the average total cost of a data breach across all industries ($3.92 million), according to Ponemon Institute.

<table>
<thead>
<tr>
<th>Year</th>
<th>Health</th>
<th>Financial</th>
<th>Energy</th>
<th>Industrial</th>
<th>Pharma</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>$65.1</td>
<td>$74.2</td>
<td>$84.7</td>
<td>$96.6</td>
<td>$110.3</td>
<td>$125.8</td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2023</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Average Total Cost of a Data Breach by Industry

Source: KBV Research

Source: Markets and Markets


**FIRM TRACK RECORD**

Capstone Headwaters’ Cybersecurity practice leverages superior industry expertise to execute a spectrum of strategic transactions in the middle market including mergers, acquisitions, recapitalizations, growth capital and specialty high yield debt, and minority and majority equity investments. Capstone Headwaters provides its clients with unique market perspectives and relationships with key decision makers among the cyber industry’s most active acquirers and investors.

<table>
<thead>
<tr>
<th>Logo</th>
<th>Company Name</th>
<th>Acquirer</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Rook Security" /></td>
<td>Rook Security</td>
<td>Sophos</td>
</tr>
<tr>
<td><img src="image2" alt="Isonas" /></td>
<td>Isonas</td>
<td>Allegion</td>
</tr>
<tr>
<td><img src="image3" alt="DGI" /></td>
<td>DGI</td>
<td>SOSi</td>
</tr>
<tr>
<td><img src="image4" alt="Idwatchdog" /></td>
<td>Idwatchdog</td>
<td>Equifax</td>
</tr>
<tr>
<td><img src="image5" alt="Solidyn" /></td>
<td>Solidyn Solutions, Inc.</td>
<td>Polaris</td>
</tr>
<tr>
<td><img src="image6" alt="GPS Source" /></td>
<td>GPS Source</td>
<td>General Dynamics Mission Systems</td>
</tr>
<tr>
<td><img src="image7" alt="Obsidian" /></td>
<td>Obsidian (A Cadmus Company)</td>
<td>Cadmus</td>
</tr>
<tr>
<td><img src="image8" alt="Cybric" /></td>
<td>Cybric</td>
<td>Capstone Ventures LLC</td>
</tr>
<tr>
<td><img src="image9" alt="Luna" /></td>
<td>Luna</td>
<td>MacB</td>
</tr>
</tbody>
</table>

---

Cybersecurity | Q2 2019
CITATIONS


**CYBERSECURITY REPORT CONTRIBUTORS**

**Tom McConnell**  
Managing Director  
tmconnell@capstoneheadwaters.com | 303-951-7125

Tom joined Capstone Headwaters in 2011 and has over 20 years of investment banking and experience with a focus on cybersecurity. Over the course of his career, Tom has completed transactions with companies across the risk management spectrum including cybersecurity technology, services, compliance, and MSSPs in both the commercial and government sectors. Tom brings a strong understanding of broader risk management having completed transactions in the physical security sector, as well. Tom began his career with a national distributor pursuing more than a dozen acquisitions, completing an S-1 registration statement for an initial public offering and arranging senior debt financing. Tom has been publicly recognized for his professional accomplishments and leadership. He received the Denver Business Journal’s Forty Under 40 award and participated in the Denver Metro Chamber of Commerce’s Leadership Denver program. In 2014, he co-founded Colorado Cyber with the mission of connecting private and public sector leaders in the cybersecurity ecosystem, stimulating discussion on critical issues, and supporting economic growth. Tom also served on the Supervisory Committee to the Board of Directors for Bellco Credit Union and the Executive Committee of the Board of Directors for Griffith Centers for Children. He is a Past President of the Denver Advisory Board. He earned his BA in Economics and Political Science for Miami University, MBA from the Daniels College of Business at University of Denver, and holds his JD in law from the University of Denver Sturm College of Law. He is a Series 63 Registered Securities Representative and Series 79 Registered Banking Representative.

**David Brinkley**  
Managing Director  
dbrinkley@capstoneheadwaters.com | 917-817-0375

David brings twenty years of experience executing over $1bn in strategic transactions for middle market firms in the Aerospace, Defense and Government sectors. David is widely recognized for his industry expertise, which encompasses intelligence and national security activities and applied advanced technologies. In addition, David holds unique security credentials that enable him to advise on the most sensitive government transactions. David also serves as a subject matter expert to the Office of the Secretary of Defense on matters pertaining to the financial health of the U.S. defense industrial base and on Pentagon-sponsored technology investments.

Prior to joining Capstone Headwaters, David founded Castellum Capital Advisors, a boutique investment bank providing advisory services to middle market firms engaged in the national security sector. Castellum Capital served as exclusive financial advisor on several high profile transactions, including large scale corporate divestitures and niche intelligence acquisitions. Prior to founding Castellum Capital, David served as Managing Director of Aronson Capital Partners, where he managed the firm’s buy and sell-side investment banking engagements. While at Aronson Capital, David completed transactions featuring prominent government services and technology firms active in international security, intelligence, and defense, with publicly-traded firms based both in the U.S. and internationally, and with leading private equity sponsors. David is a Series 63 Registered Securities Representative and Series 79 Registered Banking Representative.
Capstone Headwaters is an elite investment banking firm dedicated to serving the corporate finance needs of middle market business owners, investors and creditors. Capstone Headwaters provides merger & acquisition, private placement, corporate restructuring and financial advisory services across 16 industry verticals to meet the life cycle needs of emerging enterprises. Headquartered in Boston, MA and Denver, CO, Capstone Headwaters has 19 offices in the US, UK and Brazil with a global reach that includes over 450 professionals in 40 countries.

www.capstoneheadwaters.com