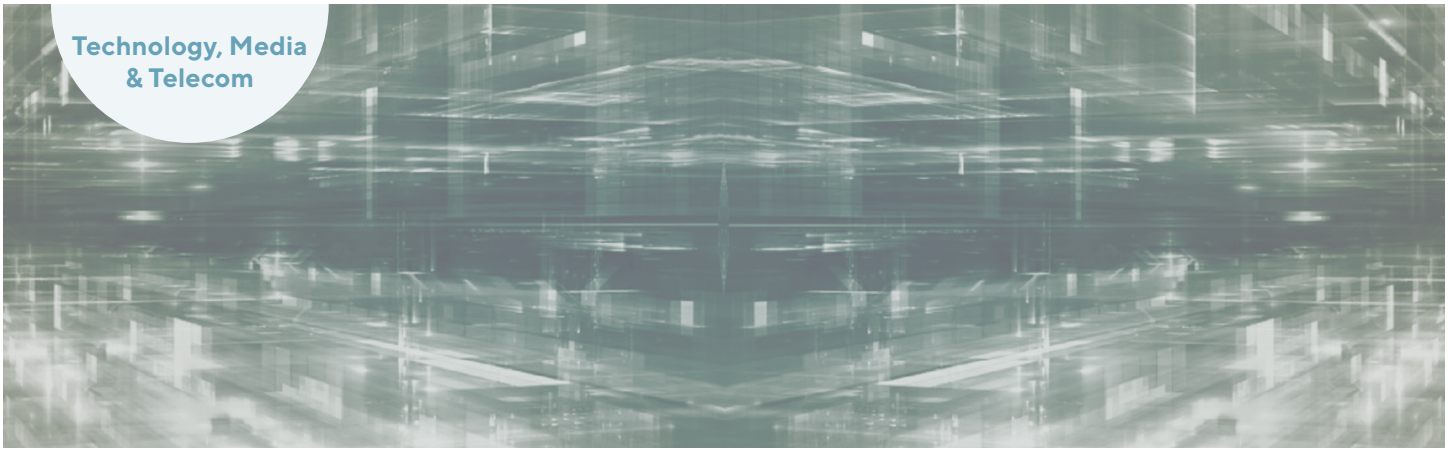

Don More, Managing Director in Lincoln International's Technology, Media & Telecom Group, recently attended Evolution Equity Partners' Annual Investor Day in New York to discuss the capital markets and cybersecurity mergers and acquisitions (M&A). At the event, Don shared his predictions for the cyber sector in 2023, which the following perspective explores in depth.

Whither Cybersecurity Deal Activity in 2023?

SECULAR DEMAND DRIVERS TO OVERPOWER MACRO HEADWINDS

Lincoln, which has completed 14 cybersecurity M&A and financing transactions since 2021, forecasts continued sector dealmaking strength in 2023, notwithstanding macro challenges, driven by healthy customer spending growth and high levels of available capital across a widening array of buyers and investors.

While cybersecurity transaction activity may decline versus 2021 and 2022 – both record years – we expect the number of acquisitions and investments to remain in line with the five-year historical average. Further, while spike valuations will be less common, and open-ended burn less tolerated, median valuation multiples should not decline materially because demand growth – the primary driver for cyber deal activity and pricing – remains robust.

Evidence supports accelerated cyber spending growth in 2023. In Q4 2022, Gartner Research predicted total sector spending growth to rise in 2023 to 11.3%, versus 7.2% in 2022. This year, for the first time, companies expect cyber to be the largest spending category in information technology budgets, according to a Spiceworks Ziff Davis survey. This is no surprise as businesses continue driving cloudification, digitalization and automation into systems and processes, creating major cyber investment exigencies.

In the course of numerous discussions with sector entrepreneurs and investors across the globe, Lincoln has found that most remain cautiously optimistic regarding 2023. Many continue to see solid pipelines, growth and customer engagement; further, strategic and financial inbound inquiries have not tailed off.

Sector spending continues to be propelled by unprecedented pressures. 2022 proved to be the most dangerous year cyber-wise on record, with no let-up expected in 2023. Microsoft detected a 130% jump in ransomware attacks in 2022, while Cloudflare found a 79% rise in denial-of-service attacks. As a result of unrest in Ukraine, cyberspace conflict and espionage rose to unprecedented levels, spilling over to major real-world shutdowns, rather than mere data theft. These include successful attacks in 2022 that halted Toyota car production, closed hospitals, caused flight delays in 50 countries and took Costa Rica's government offline.

In response, 2023 will see further imposition of regulatory requirements from government entities worldwide, catalyzing further cyber spending. In 2022, the U.S. Securities and Exchange Commission proposed mandatory 8-K reporting of material cybersecurity incidents within four business days, and disclosures on company policies to manage cybersecurity risk. The UK added strict security rules to its existing Telecommunications (Security) Act. The European Commission also proposed new cybersecurity rules to create a framework for governance, risk and compliance.

(continued on next page)

LINCOLN PERSPECTIVE

Lincoln sees particularly strong investor and strategic interest in cybersecurity vendors who address one or more of the below needs.

- Hardening of multi-cloud / hybrid infrastructure and applications
- Extended detection and response operationalization in security operations centers and managed detection and response
- Continuous security visibility and monitoring across the digital estate
- Identity credentials exploitation and theft prevention
- Protection of rapidly expanding and diversifying endpoints
- Incorporation of artificial intelligence into threat intel, detection and incident response
- Next-generation authentication management for greater scalability and reduced fraud
- Vulnerability management of operational technology networks, internet of things and machines
- Resilience development / disaster recovery through enhanced early detection and containment
- Enhanced cyber risk quantification
- Cloud data governance and compliance management
- Application programming interface and supply chain security
- Zero-trust network access

The cybersecurity market is fragmented and will remain so for the foreseeable future, given the dynamic complexity of the threat environment. That said, consolidation will continue apace within major subsectors – such as identity and access management, vulnerability management and secure access service edge — as larger vendors seek complete solutions and enhanced growth.

Though building new products is an option, publics and late-stage private equity-backed players in the sector have proven more effective at selling rather than innovating, and prefer the one-time capital expense of acquisitions to speculative research and development investments that reduce operating margins. Further, numerous financial sponsors that Lincoln speaks with regularly indicate that they seek to deploy capital in cyber. Consequently, the flywheel of security investment and M&A, pushed by rapid technology and threat evolution, will continue at a healthy pace in 2023.

Learn more about Lincoln International's Technology, Media & Telecom Group and connect with the team at www.lincolninternational.com/whoweserve/technology.