Cybersecurity: Zeroing in on Current and Future Trends

As we enter the second half of the year, the state of cybersecurity is coming into sharper focus following a tumultuous 2022. Here are Lincoln International's key observations and predictions.

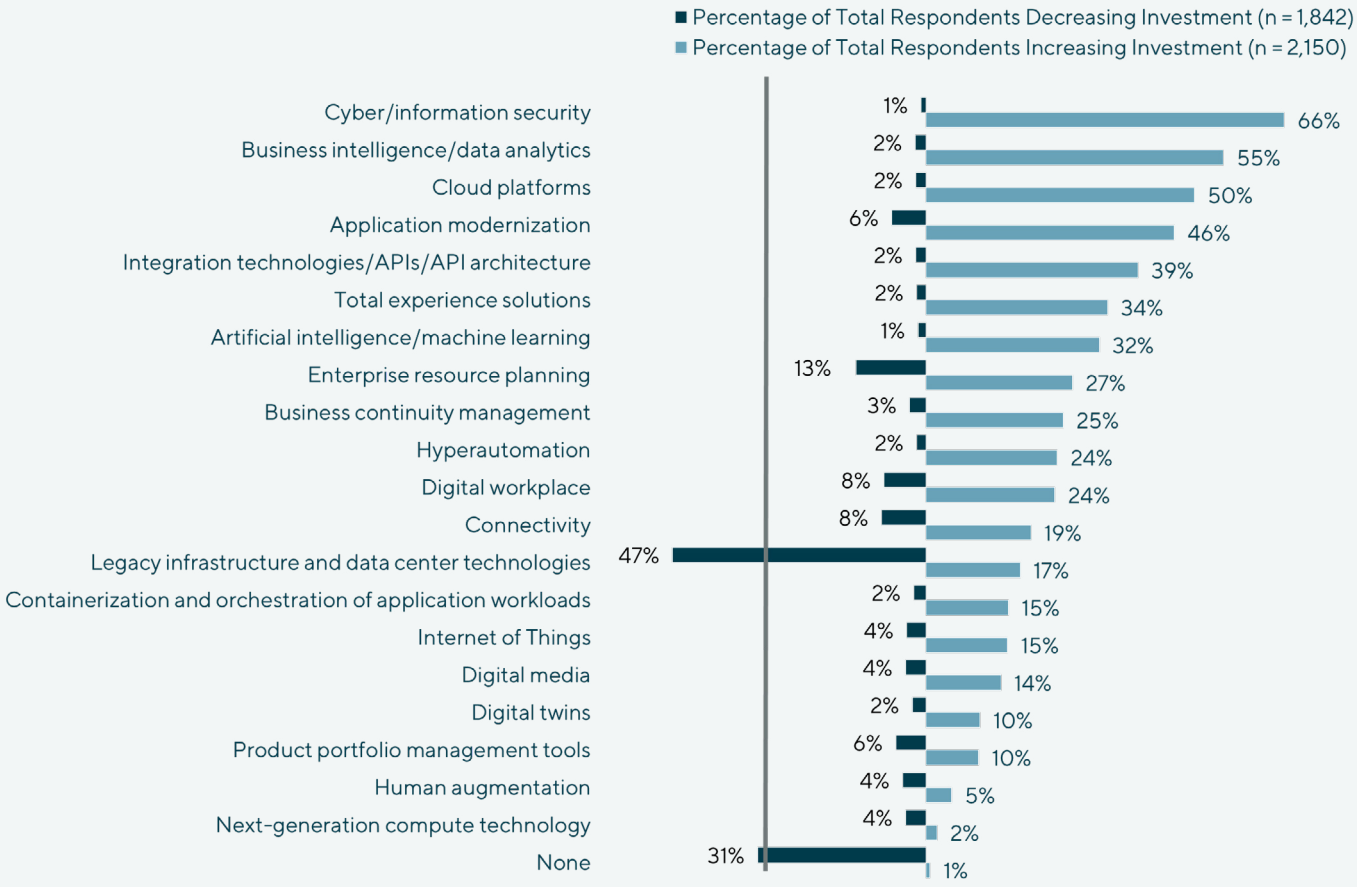
> ***Cybersecurity remains the number one technology investment priority for organizations***

Deal Market Thawing Following a Slow Start to 2023

As reported in our Q1 quarterly report, mergers and acquisitions (M&A) and investment volumes, while down, remained relatively healthy in comparison to historical averages (excluding 2021) and are gradually rising again. As a sentiment barometer, April's RSA conference had a distinctively positive vibe with buzzy crowds and overflowing social events. Anecdotally, Lincoln's Cyber CEO dinner at RSAC, attended by close to 50 vendors, struck an optimistic tone concerning demand, pipelines and inbound strategic / financial interest. Cybersecurity remains the number one technology investment priority for organizations, as shown by a recent Gartner executive spending survey (figure 1).

(continued on next page)

Figure 1



Source: 2023 Gartner CIO and Technology Executive Survey

Deal Thaw will Accelerate in 2024

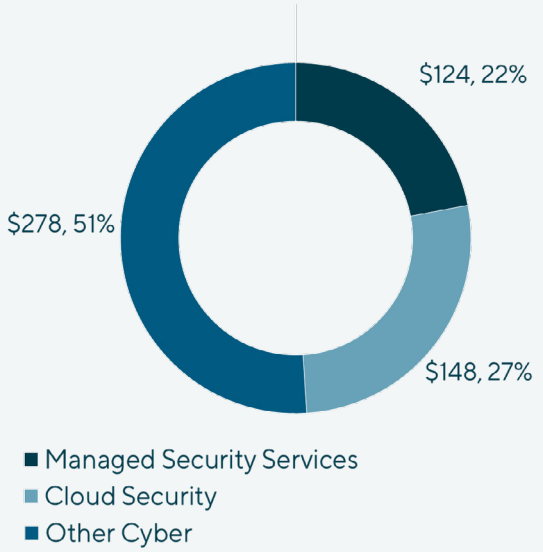
We see the pipeline of M&A and investment processes preparing to go to market lengthening, and our market checks show definitive itchiness by investors and strategics to deploy capital. Further, as we reported in Q1, the pool of cyber buyers (as defined by the number of relevant strategics with > $100 million revenues) has expanded by 75% over the past three years, reflecting the impact of $165 billion of expansion capital deployed by investors and acquirers in cyber just since 2021. There is also a record number of initial public offering-worthy cyber unicorns (>50) waiting in the wings for the public capital markets to reopen, creating a new pool of growth capital and liquid stock for further acquisitions.

(continued on next page)

Intensifying Vendor Collaboration to Benefit those with Partnering Virtuosity

RSAC's 'Stronger Together' theme alludes to the value of alliances, more of which were announced than at any prior RSA conference. Presenters spoke of a pressing need for integration across three capability spectrums: visibility (endpoint, network and cloud), time (before, during and after attack) and function (human / manual – AI / automation). CrowdStrike emphasized increasing attack sophistication as necessitating the embrace of a holistic, shared approach to security. Cisco discussed the value of information-sharing among vendors, government and cyber professionals to address the evolving threat landscape. Accenture announced an alliance with Palo Alto Networks to combine extended detection and response, AI and know-how. In addition to placing a premium on vendors that play well with others, it also benefits those with unified platform offerings.

Figure 2



Sources: Allied Market Research, Market.us, Transparency Market Research and Fortune Business Insights

(continued on next page)

M&A Consolidation to Accelerate Within, Rather than Across, Segment Stacks

While surveys suggest that organizations seek to reduce the number of cyber vendors they utilize, the goal is not cost-cutting, but greater efficacy. Consequently, we see acquisitions focused on creating function-defined platforms – resulting in category powerhouses, rather than supermarket-style consolidators like the Symantecs and McAfees of the olden days. Platform stack leaders are forming in areas that notably include cloud workload security, data security, attack surface management, identity and access management, security service edge, extended detection and response and integrated risk management.

Managed Security Services and Cloud Security to Dominate M&A and Investment Activity

Within a decade, we estimate that half of total annual cyber spending will run through managed security services and cloud platforms (see figure 2). Hence, acquirer and investor activity will be over-indexed toward these areas. In managed security (managed detection and response / managed security service providers) for example, billions of dollars in anchor private equity investments have been made recently to create and grow platforms (e.g., ArcticWolf, Avertium, BinaryDefense, Blackpoint, BlueVoyant, CriticalStart, DeepWatch, eSentire, Expel, Red Canary and ReliaQuest). This is similarly seen in big investments in cloud-based security platforms (e.g., Apiiro, CipherCloud, Coro, Lacework, Netscope, Panther Labs, Orca, Snyk and Wiz).

AI Emergence in Cyber is Real and Rapid

AI was the most ubiquitous discussion topic, both at RSA 2023 and June's Gartner Security & Risk Summit, revolving around how vendors and customers plan to integrate it into their cyber planning. While concerns surrounding AI's benefits to cybercrime are great, the consensus is that the new capabilities will be a net positive for enhancing threat detection and incident response. Annual global spend on AI-based cybersecurity products is predicted to reach $97 billion by 2032, and will be seen largely in the form of solution upgrades rather as new security categories or AI-pure plays. This will energize replacement and upsell cycles. We see vendors already including AI plans in development roadmaps as more than 70% of organizations will have generative AI embedded into security operations within the next five years.

> ***The consensus is that the new capabilities of AI will be a net positive for enhancing threat detection and incident response.***

Rule-of-40 has Permanently Displaced Revenue Growth as the Industry's Primary Value Driver and Correlator

For more than a decade until late 2021, the cyber industry's strongest predictor, by far, of vendor valuation (utilizing R-squared coefficient of determination), was short-term projected revenue growth. For example, a scatterplot of publicly traded cyber vendors' enterprise value / next-year estimated revenues versus next-year estimated revenue growth rates routinely generated R-squared values exceeding 0.7. This means that greater than 70% of a cyber vendor's value was determinable by its near-term revenue growth rate. Performing the same analysis using Rule 40% rather than revenue growth (enterprise value / next-year estimated revenues versus [next-year estimated revenue growth rate + EBITDA margin]) resulted in a much lower correlation, typically in the 40% range, meaning that EBITDA profitability actually reduced valuation multiples. Today–and this has been the case for over a year–the correlations are reversed, so that Rule of 40%, which considers profitability, is a much better predictor of valuation than revenue growth alone (see figure 3). The significance of this shift is that future investments will be geared toward driving profitability, even at the expense of growth. This is seen in the sharp change in public vendor performance just since last year. In 2022, three of 25 U.S. publicly traded cyber vendors were EBITDA-positive, and in 2023 the Street projects that 23 of 25 of these vendors will be profitable, while median annual revenue growth is expected to halve. The implications are already being seen in the private markets, with investment capital shifting to support near-profitable and cash-flow-positive cyber businesses. This has resulted in lower revenue valuation multiples as well as lower revenue growth rates as companies retool operations; these multiples however will stabilize and start rising as more companies turn profitable and funnel cash flow to more durable growth models.

(continued on next page)

Figure 3

Revenue Growth versus Enterprise Value / Revenue Multiples

Rule of 40[1] versus Enterprise Value / Revenue Multiples

Source: Market data sourced from S&P Capital IQ as of 05/10/2023

(1) The Rule of 40 is calculated as 2023 projected revenue growth plus 2023 projected EBITDA margin

For other perspectives, visit us at www.lincolninternational.com/perspectives.

Get to know Lincoln's Global TMT Group at www.lincolninternational.com/technology.