All Systems Protected? Cybersecurity Trends in 2022

Accelerated digitalization post-COVID-19, convergence of cyber and military power projection and the increasingly complex threat environment are forcing rapid transformation of the cybersecurity industry. Organizations are hungry to protect systems and people from unprecedented dangers. A single ransomware attack, data breach or malware penetration can take down a company – or even a country. The dangers are felt directly as never before as geopolitical conflicts spill over into the cyber realm – and from the battlefield to the board room. Inevitably, the demarcation line between military and civilian targets is blurry. We are all in the blast radius of the next cyber war. The stakes have never been higher, and complacency is no longer an option.

This urgent call to arms creates unprecedented opportunities for vendors heeding the call for a new generation of smarter, faster, continuous and resilient security solutions. Consequently, savvy entrepreneurs, investors and strategic acquirers are looking out toward the high-growth horizon – beyond short-term, macro-driven market volatility – to the new cyber frontier. In a recent survey conducted by Lincoln International, more than 70% of senior security executives say they expect mergers and acquisitions (M&A) activity to increase and valuations to remain the same or rise. In fact, the first-half of 2022 has seen near-record transaction volumes with relatively modest deal multiples compression. Further, the vast majority of cyber publics met or beat analyst projections in Q1 and Q2. The take-private of 11 public vendors since 2021 by private equity firms supports the view that short-term share price dips will likely not hold.

Lincoln believes that all of this points to elevated levels of investment and M&A activity in the cybersecurity sector, as well as healthy valuations for the foreseeable future. There is neither a shortage of cybersecurity capital or customer demand – only innovation is scarce, and the world needs a lot of it.

Further, based on Lincoln's discussions across the globe and activity (we've closed 11 cyber M&A transactions since the start of 2021), we see several themes resounding across the cybersecurity community. As noted, confidence in the strength of the cybersecurity market remains high. We also see an over-indexing toward investment in all things public cloud security related, education and training, continuous identity protection, managed detection and response (MDR), extended detection and response (XDR), secure access service edge (SASE) and zero trust framework adoption.

XDR

As leading vendors continue broadening their platforms to improve efficacy and efficiency, XDR is becoming a critical capability signifying unified detection and response to threats across endpoints, networks and the cloud.

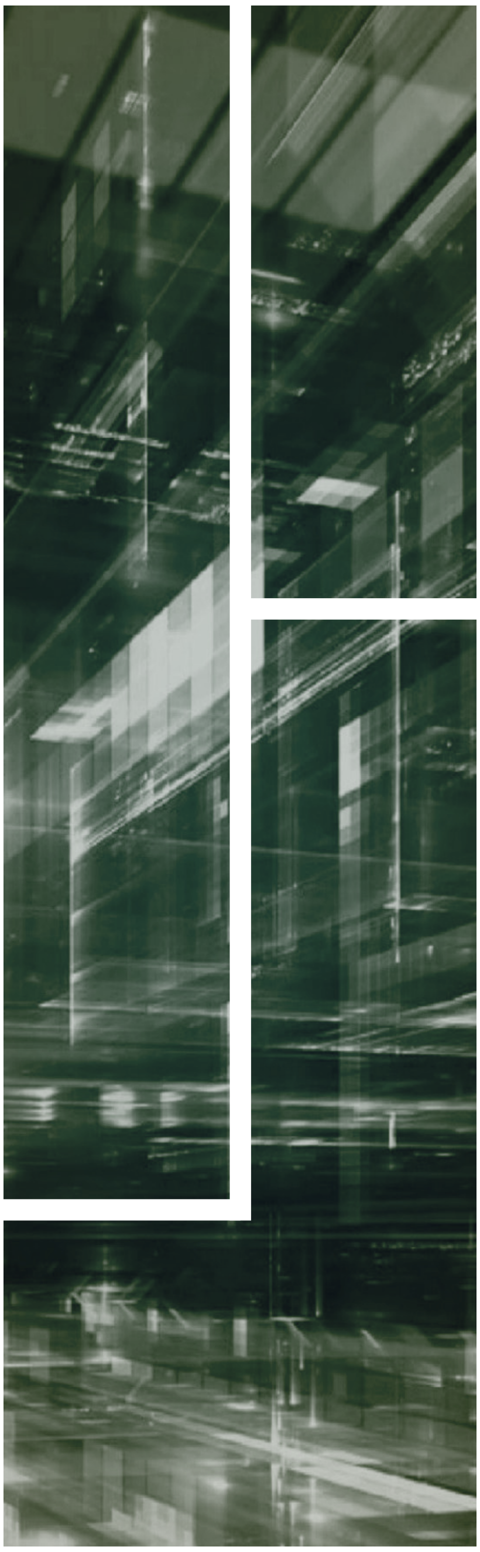
XDR solutions combine network detection and response (NDR), endpoint detection and response (EDR), identity threat detection and response (ITDR) and security orchestration, automation and response (SOAR) capabilities into a single, cohesive incident detection and response platform. This makes it far easier for security teams in-house, or external managed detection and response (MDR) vendors to neutralize advanced threats.

While vendor consolidation is not a new trend, solution complexity continues driving emergence of integrated platforms. We expect this trend to accelerate and leading vendors to morph into integrated solution providers, which will drive consolidation of specialized players.

CYBER IS ALL ABOUT SKILLS AND SERVICES

A worsening global shortage of skilled cybersecurity personnel is driving high demand growth for training solutions, both for professionals and employees, and for managed services (outsourcing). Lincoln's recent cybersecurity survey found the cyber skills and education gap to be the biggest challenge facing organizations near term. Further, Gartner Research predicts that, by 2025, more than 50% of organizations will utilize managed security services for their cyber needs – in part reflecting the inability to hire skills in house, but also reflecting the cost benefit of outsourcing.

Managed security service providers (MSSPs) are morphing into MDRs, which leverage proprietary or 3d-party XDR to provide full visibility into threats and enable rapid response to breaches. Complexity, cost and skills shortage considerations have made MDR vendors offering outsourced, managed "Security as a Service" the strongest area of cyber interest for PE firms.



(continued on next page)

CLOUD-FIRST IS THE DOMINANT PARADIGM

On-premise computing and security is taking a back seat to the cloud, a trend which COVID-19 accelerated. Today, more than 90% of enterprises are turning to cloud infrastructure platforms to run at least part of their operations. Consequently, securing modern cloud workloads is now at the center of every cybersecurity strategy.

Cloud security posture management, cloud workload protection platforms, cloud access security brokers and kubnernetes security are cornerstones to running safely in cloud environments. Almost all cyber spending growth going forward addresses in some way the challenge of securing cloud access, applications, operations and data.

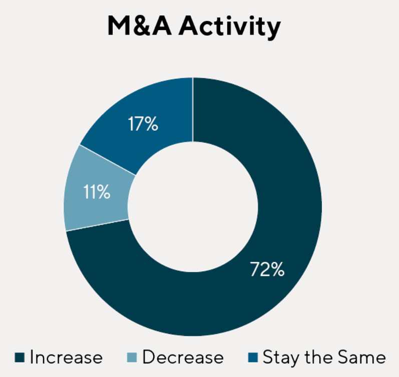
THE NEED TO RETHINK IDENTITY AND RISK TO UNLOCK POTENTIAL OF THE CLOUD

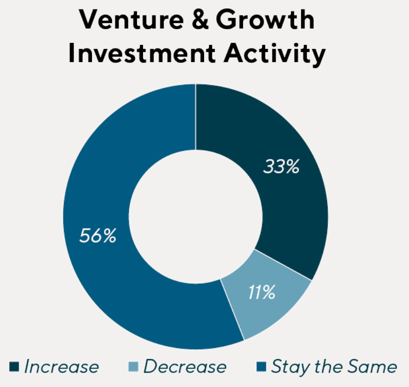
Although identity and access management is not a new segment of cybersecurity, broad acceptance of the zero trust framework requires continuous authentication, access provisioning and risk assessment across the IT environment of users, applications, data stores, containers, secrets and cloud services. The industry is also actively pursuing machine identity management solutions for connected vehicles, sensors and other IoT devices.

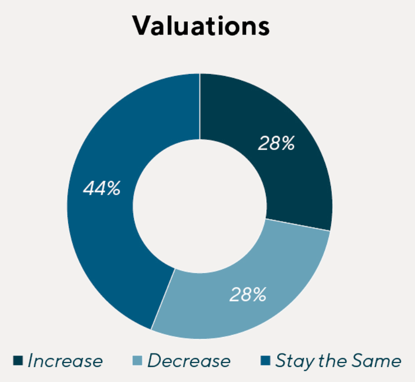
Related areas integral to enabling secure operations across hybrid cloud environments include digital supply chain security, third party risk management, cloud data governance and external attack surface management.

Summary Findings from Cybersecurity Survey

A recent Lincoln survey of leading cybersecurity professionals found optimism despite market headwinds. Two-thirds of respondents actually expect sector M&A activity levels to increase further over time. Most also believe that venture and growth investment will remain at current levels or go higher. Additionally, most expressed the view that valuations would remain the same or go even higher.



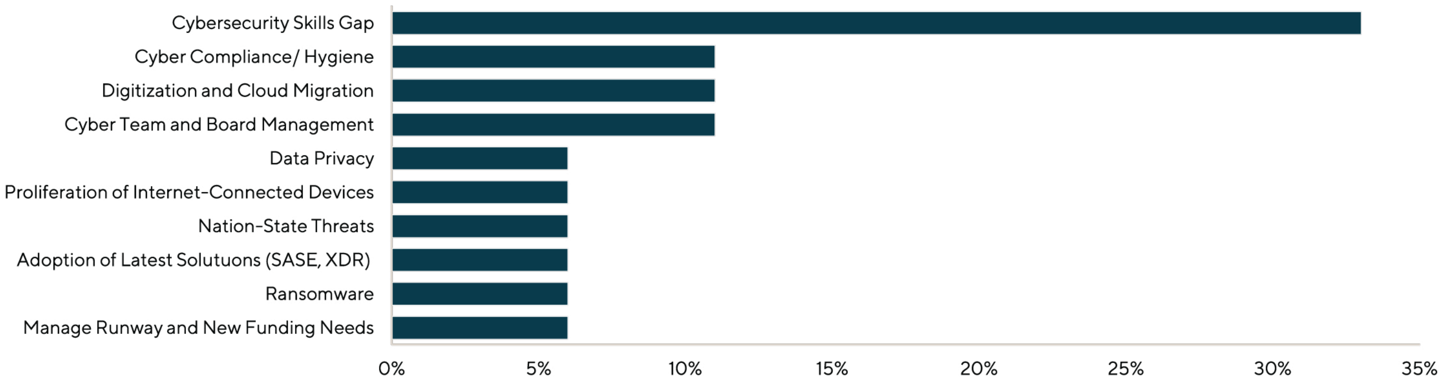


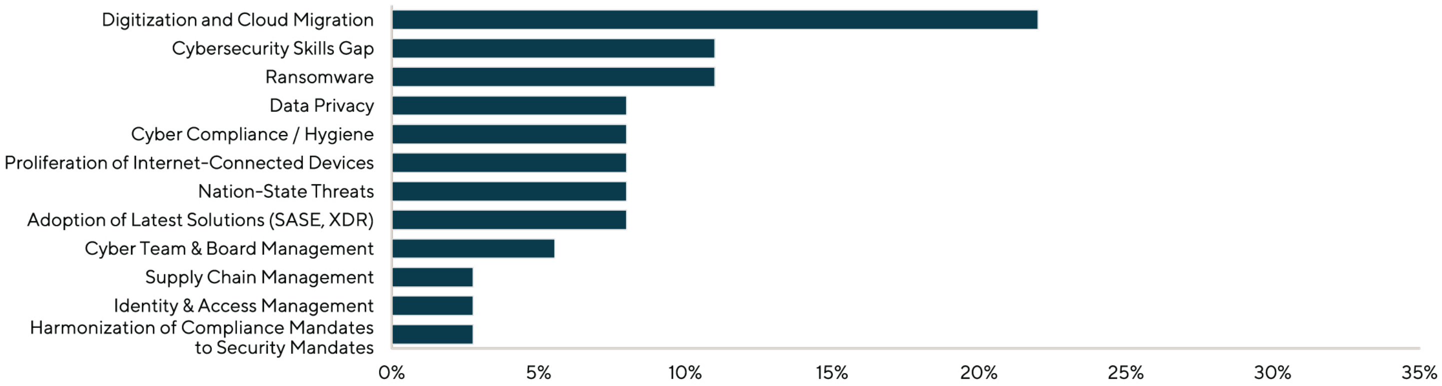


When asked what challenges they expect cybersecurity organizations to face in the near term, more than a third of respondents put the cybersecurity skills gap on top of their list, followed by compliance and challenges related to the shift to cloud, in line with the key topics and trends identified below.

Which are the main challenges cybersecurity organizations face over the next three months?

Ranked as #2-3 Challenge





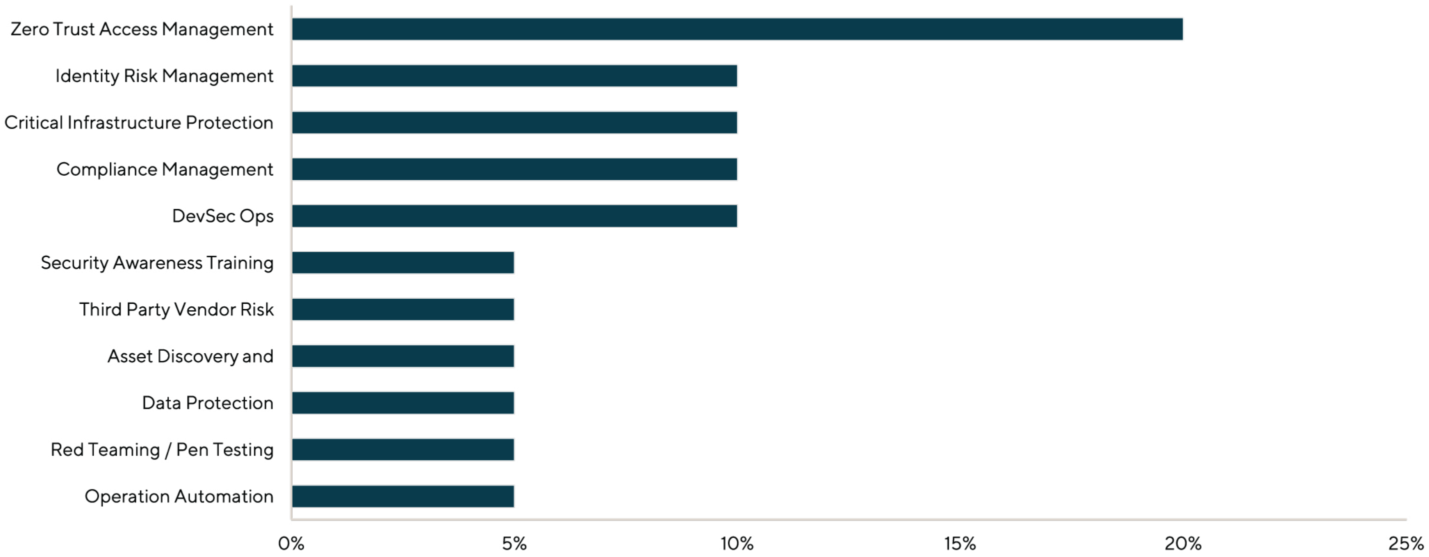
share of respondents (%)

(continued on next page)

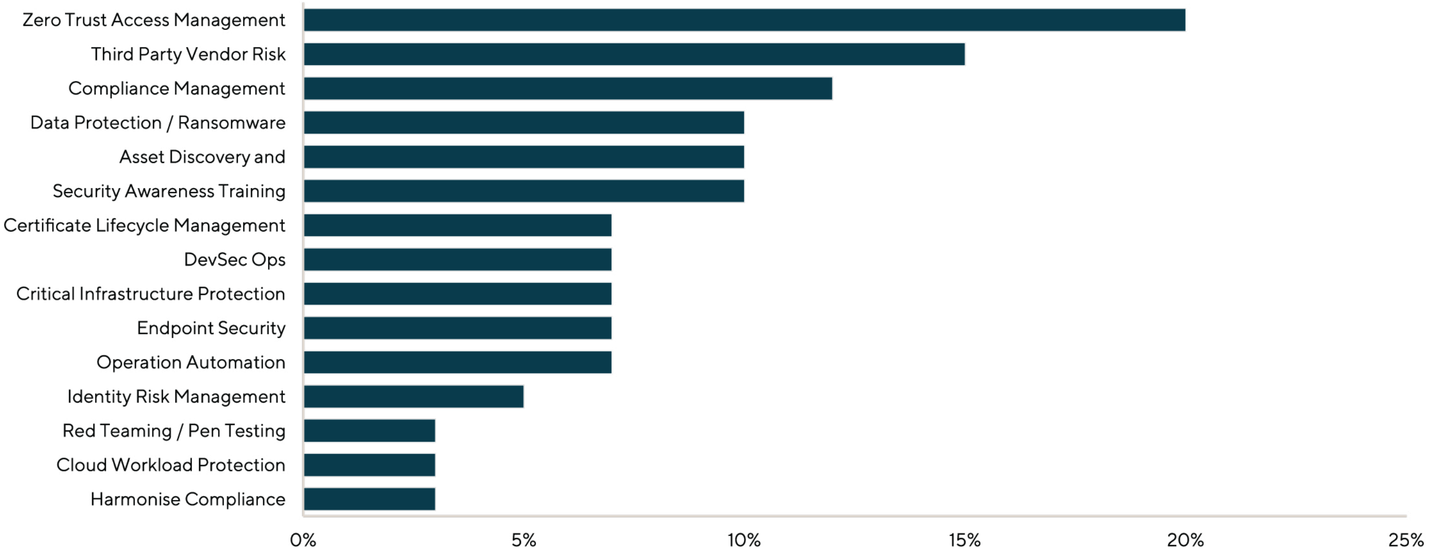
Unsurprisingly, most respondents believe that investment in zero trust and critical infrastructure protection is integral to improving organizations' cybersecurity posture. Other areas of priority include third-party vendor management, compliance management and data security.

Which areas should organizations prioritize to improve their cybersecurity posture?

Ranked as #1 Priority



Ranked as #1-3 Priority



Interested in other perspectives on the cybersecurity industry? Sign up to receive email updates to stay on the pulse of what is happening in the sector.

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