

Albany Investment - Monthly Update – March 2025

Cybersecurity M&As:

Alphabet/Wiz

- Alphabet (GOOGL) announced its agreement to acquire cybersecurity firm Wiz for \$32 billion (18 March 2025), all in cash.
- This marks Alphabet's largest acquisition to date and aims to enhance Google's cloud computing and security offerings, expecting to bolster Google's competitiveness in the cloud services market against rivals like MSFT and AMZN, solidifying their market position.
- Through integration, Google aims to provide an end-to-end security solution which simplifies cybersecurity for organisations of all sizes.¹
- Google's decision to acquire Wiz, rather than developing similar technology in-house, represents a faster, safer, and more strategic move. This acquisition immediately strengthens Google Cloud's security, brings in top-tier cybersecurity talent, and prevents competitors from gaining an edge. Additionally, it accelerates innovation while reducing development risks and costs, essentially 'shortcutting' the expenses and time required for in-house development.

ServiceNow/Move works

- ServiceNow has agreed to acquire Moveworks, an enterprise AI and automation platform, in a \$2.85 billion cash and stock deal (10 March, 2025). This acquisition integrates Moveworks' AI assistant and enterprise search with ServiceNow's automation capabilities, aiming to enhance productivity and streamline enterprise interactions.¹
- The move strengthens ServiceNow's competitive position against players like Salesforce by offering AI-driven solutions across sales, fulfilment, and service functions.
- While post-acquisition integration will require careful planning, this investment underscores ServiceNow's commitment to AI innovation.
- Rather than developing the technology in-house, acquiring Moveworks provides an instant AI upgrade, secures top AI talent, reduces development risks, and blocks competitors from gaining an edge, accelerating AI-powered automation at scale.
- Moreover, while \$2.85 billion is a significant investment, it 'shortcuts' R&D costs, hiring expenses and the uncertainty of developing a comparable solution in house.
- This acquisition ensures a faster Return on Investment, by enabling quick deployment and wider market adoption.

Other:

- **Turn/River Capital** Private Equity Firm Turn/River capital agreed to acquire SolarWinds, a provider of IT management solutions, for approximately \$4.4 billion in cash. This move will transition solar winds into a privately held company.³
- **CyberArk/Zilla Security:** CyberArk, a leader in identity security, announced the acquisition of Zilla Security, an Identity Governance and Administration (IGA) vendor, for \$165 million in cash (February 2025). This acquisition is expected to enhance CyberArk's Identity Security Platform by automating processes like compliance reviews.³
- **Sophos/Secureworks:** Cybersecurity firm Sophos finalised its acquisition of Secureworks (February 2025), a company specialising in extended detection and response (XDR), at a value of \$859 million. This acquisition aims to enhance Sophos' product offerings and expand its presence in the managed security services sector.¹

Industry Trends:

Strong M&A activity in the cybersecurity sector driven by the need to address increasing cyber threats, regulatory compliance demands and the necessity of integrates security solutions.

Strategic Acquisition drivers:

- **Expansion Capabilities:** As firms acquire niche companies to enhance offerings in areas such as identity and access management (IAM), cloud security, and AI-driven threat intelligence.
- **Competitive Advantage:** M&A helps companies scale, expand market share, and build customer trust faster than organic growth, due to the speed of integration, 'shortcutting' R&D and allowing companies to integrate with proven technologies seamlessly, rather than investing years in developing frameworks.
- **Investor Confidence:** Private equity firms are investing in cybersecurity due to its strong growth, recurring revenue models, and increasing regulatory demand. SaaS-based security solutions offer predictable cash flows, while M&A activity by tech giants creates lucrative exit opportunities. The fragmented market allows PE firms to acquire and consolidate smaller players, boosting efficiency and valuations.²

Challenges in M&A:

- **High Valuations:** Intense competition for leading cybersecurity firms is driving up acquisition costs, as major tech companies and private equity investors vie to enhance their security portfolios amid escalating cyber threats. This competitive landscape results in elevated valuations, making deals more expensive and financially complex.
- **Regulatory Scrutiny:** Governments and regulatory bodies closely monitor cybersecurity acquisitions due to concerns over data privacy, national security, and potential market monopolisation. Cross-border deals face heightened scrutiny, especially when they involve sensitive infrastructure or consumer data protection laws like GDPR and CCPA. E.g.

¹ <https://www.securityweek.com/cybersecurity-ma-roundup-28-deals-announced-in-february-2025/>

² <https://www.reuters.com/markets/deals/buyout-firms-vie-cybersecurity-firm-trend-micro-sources>

Google/Wiz is anticipated to undergo rigorous regulatory examination given its scale and the current focus on BigTech's market influence.³

- **Post merger Integration:** Merging cybersecurity firms necessitates the seamless integration of technology infrastructures, security protocols, and corporate cultures, which can be intricate and time-consuming. Misalignment in these areas may lead to operational inefficiencies, security vulnerabilities, and customer dissatisfaction due to potential service disruptions.

Cyber Security Threat Developments:

- **State Sponsored Espionage:** North Korean hackers hacked one of ByBit's suppliers to secretly alter the digital wallet address that 401,000 Ethereum crypto coins were being sent to, ByBit thought it was transferring funds to its own digital wallet, but instead sent it to hackers. \$300mn of the total hack value of \$1.5bn in crypto is thought to have been successfully converted into unrecoverable funds, potentially to be used in North Korea's defence budget.³
- **Termination of CIPAC Raises Concerns:** The U.S. Department of Homeland Security's recent termination of the Critical Infrastructure Partnership Advisory Council (CIPAC) has raised concerns within the cybersecurity community about weakened public-private sector trust and increased vulnerability to cyber threats. CIPAC facilitated secure exchanges of threat intelligence between private companies and federal agencies.⁴
- **AI Powered Cyberattacks:** Hackers are increasingly using artificial intelligence (AI) to enhance cyberattack capabilities. At the HumanX Conference in Las Vegas (2024), experts highlighted the risk of AI-driven autonomous cyberattacks capable of bypassing traditional security measures. Notably, a recent DeepLocker-style malware demonstrated how AI could be used to evade detection until reaching a specific target.⁵
- **Europol Reported Increased Sabotage Activities:** Europol's recent report highlights a surge in politically motivated cyber-attacks and sabotage within the EU, driven by alliances between state actors like Russia and organized criminal gangs. These activities aim to destabilize the region and include cyber-attacks, data theft, and other criminal endeavours.⁶
- **Ransomware Evolution:** The rise of ransomware as a service (RaaS) has lowered the barrier to entry for cybercriminals, enabling even low skilled attackers to deploy sophisticated ransomware tools. A notable example is the Black Basta ransomware group, which has targeted organisations across healthcare, manufacturing and financial services. In response, AI-Driven threat intelligence and automated response systems are becoming essential for mitigating ransomware risks.⁷

³ <https://www.bbc.co.uk/news/articles/c2kgndwwd7lo>

⁴ <https://www.axios.com/newsletters/axios-future-of-cybersecurity-15029f10-00fb-11f0-9b3b-518d00b5835d>

⁵ <https://www.axios.com/2025/03/14/hackers-artificial-intelligence-cyber-threats>

⁶ https://www.ft.com/content/755593c8-8614-4953-a4b2-09a0d2794684?utm_

⁷ https://www.ft.com/content/3b172a2a-4be5-4ef4-87cb-7fdcdee2ad99?utm_source=chatgpt.com