ALBANY INVESTMENT

Albany Investment - Monthly Update – June 2025

Cybersecurity M&As:

In June 2025, 41 cybersecurity M&A deals were announced globally,[1] marking a strong month for the industry with trends of consolidation and increasing AI usage:

- **Bitdefender**, a global cybersecurity leader, is set to acquire **Mesh Security** (18th June), aiming to integrate Mesh's advanced email security solutions to strengthen Bitdefender GravityZone, the firm's flagship security, compliance, and risk analytics platform.[2] This acquisition has arisen amid a landscape of increasing email exploitation, with the FBI reporting ~$2.8bn losses from business email compromise (BEC) scams alone.[3]
- **Cellebrite**, an Israel-based forensic investigation solutions provider, has agreed to acquire **Corellium** (5th June) for $200mn, with $170mn in cash up-front, and the remaining portion in equity, subject to performance milestones over the next two years.[4] The acquisition will 'accelerate the identification of mobile vulnerabilities and exploits,' as Correlium's virtual device platform eliminates the need for physical hardware.[5]
- **Cyera**, the world's fastest-growing data security company in history, has accelerated its growth with the acquisition of **Otterize** (26th June), a platform for securing cloud-native non-human identities and data flows, to tackle cloud identity sprawl.[6]
- **NETGEAR** announced a definitive agreement to acquire **Exium** (5th June), a cybersecurity company providing Secure Access Service Edge (SASE) solutions, as part of continued investments in cloud-based solutions for advanced networking capabilities. NETGEAR's integration efforts enable it to take advantage of a booming SASE market, with Gartner estimating a 29% CAGR and a market size of over $25bn by 2027.[7]
- **OneSpan**, formerly Vasco, a leading identity solutions provider, has acquired passwordless software authentication firm **Nok Nok Labs** (5th June) following a previous partnership in 2018.[8] The acquisition enables OneSpan to provide industry-leading, future-ready authentication flexibility to customers, with Nok Nok's leading FIDO solutions complementing OneSpan's recently launched FIDO2 security keys.[9]
- **Rubrik**, a SaaS data backup platform vendor, has announced its intention to acquire AI specialist, **Predibase** (25th June), for over $100mn, creating a respected team of Google and Uber AI alumni to drive agentic AI adoption globally, unlocking value for clients.[10]
- **Securonix**, a dominant security information and event management (SIEM) platform provider, has acquired **ThreatQuotient** (11th June), known for its renowned ThreatQ detection, investigation, and response (TDIR) offering.[11] The acquisition will boost Securonix' plans to create a fully integrated AI-driven security operations platform.[12]

[1] Cybersecurity M&A Roundup: 41 Deals Announced in June 2025
[2] Bitdefender to Acquire Mesh Security, expanding its email security capabilities
[3] Bitdefender to acquire Mesh, enhancing email security platform
[4] Paladin Capital Group portfolio company Corellium enters into agreement to be acquired by Cellebrite
[5] Cellebrite to acquire mobile testing startup Corellium
[6] Cyera acquires Otterize to expand its data security platform
[7] NETGEAR acquires Exium for integrated networking and security
[8] OneSpan acquires Nok Nok in FIDO authentication drive
[9] OneSpan accelerates FIDO leadership with acquisition of Nok Nok Labs
[10] Rubrik to Acquire Predibase to Accelerate Agentic AI Adoption
[11] Securonix acquires ThreatQuotient to deliver industry's broadest and deepest TDIR
[12] Securonix acquires ThreatQuotient to deliver unified threat intelligence and AI-Powered SIEM

- **Synk**, a leader in secure AI software development, announced the acquisition of **Invariant Labs** (24th June), a globally recognised deep-tech spin-off from ETH Zurich. The deal integrates Invariant's pioneering AI safeguarding into Synk's recently launched AI Trust Platform, to help customers protect against current and emerging threats.[13]

Cybersecurity Developments:

- Global Data Breaches and Cyber Attacks: **IT Governance** found 33 publicly disclosed cybersecurity incidents, including the leak of 16bn user credentials, and excluding this mass credential dump, over 23mn records were compromised. This mass data breach is one of the largest in history and includes login information for many online services. Healthcare is the industry that has been most affected, with notable cases including 5.4mn records at **Episource**, 743k records at **McLaren**, and 730k records at **Kettering**.[14]
- UK Retail Cyber Attacks: In recent months, **Adidas**, **Harrods**, **H&M**, **M&S**, and **Co-op** have suffered cyber attacks or major IT outages, but M&S have partially resumed online orders (10th June), and four people were arrested, who were believed to be associated with 'Scattered Spider,' a group that likely worked in cooperation with ransomware group 'DragonForce' to conduct the cyber attacks.[15] The **Cyber Monitoring Centre** (CMC) has classified the UK Retail Cyber Attacks as a 'Category 2 Systemic Event' with a 'narrow and deep' impact that has caused an estimated total financial effect of between £270mn to £440mn, which led to the equivalent of a 30% hit to M&S' profits.[16]
- 23andMe Fines: The Information Commissioner's Office has fined genetic testing company **23andMe** £2.31mn (17th June) for failing to implement appropriate security measures to protect the personal information of UK users, following a cyber attack in 2023 and notice of intent to fine in March that had envisaged a higher £4.59mn fine.[17]
- UK Cybersecurity Legislation: The **UK Government** published the Cyber Security Growth Action Plan (18th June), which will examine the strength of the UK's cyber sector, with a current annual revenue of £13.2bn, and provide recommendations to unlock more jobs, support innovation, and drive forward the government's Plan for Change, while feeding into the forthcoming National Cyber Strategy, which aims to sustain the UK's competitive position in an interconnected world.[18]
- Israel-Iran Spillover Effects in Cyberspace: **Radware** published a threat alert (18th June) that found that 'government-backed hackers, patriotic hacktivists, online propagandists, and opportunistic cybercriminals have all been active,' following a cyber attack on Iran's **Bank Sepah** (17th June) and theft of $90mn from Iran's **Nobitex** (18th June), as well as fraudulent text messages up 700% to create panic in Israel.[19]
- UK Cyber Training Scheme: The Prime Minister launched a £187mn **TechFirst** scheme (9th June) to train over 7mn UK workers in essential AI skills following a DSIT report that by 2035, ~10mn workers will be in roles involving AI, and 1mn young students as part of **TechYouth**, backed by £24mn of government funding.[20]

[13] Synk acquires Invariant Labs to accelerate Agentic AI security innovation
[14] Global Data Breaches and Cyber Attacks in June 2025: Over 16 billion records exposed
[15] What can I buy online at M&S since the hack?
[16] Cyber Monitoring Centre Statement on Ransomware Incidents in the Retail Sector – June 2025
[17] 23andMe fined £2.31 million for failing to protect UK users' genetic data
[18] Cyber Growth Action Plan 2025 – Policy Paper
[19] Hacking, crypto, and destroying data: How the Israel-Iran conflict is developing in cyberspace
[20] PM launches national skills drive to unlock opportunities for young people in tech