

J&A Sell-Side M&A Report

Cybersecurity, Governance, Risk and Compliance Services Sector M&A Transactions and Valuations

March 2026

AUTHORS



RIM CHAABAN

Rim is based in J&A's Abu Dhabi office and is a member of the investment banking team. She is an associate at J&A and is responsible for providing investment banking advisory services to clients including but not limited to memorandum drafting, valuation analysis, comparable analysis, financial statement analysis, and financial statement forecasting. She holds a bachelor's degree in business administration with a focus on accounting and finance.



JOSHUA JAHANI

Joshua Jahani is a managing director at Jahani and Associates. He is based in the New York City office. He leads the firm's global expansion and client service activities. He has been featured in over 50 publications such as the BBC, Newsweek, International Business Times, NBC, and more about investment banking and global trade. Joshua is a lecturer at Cornell University and New York University, and is a published author with John Wiley and Sons for his book, *Data Driven Decisions*.



From Q1 2021 through Q4 2025, escalating cyber threats, expanding regulatory mandates, and rising enterprise digital exposure drove sustained M&A activity across the cybersecurity, governance, risk, and compliance (GRC) services sector. As organizations accelerated cloud adoption, AI deployment, and broader digital transformation initiatives, security and compliance functions became deeply embedded within core IT infrastructure and enterprise risk management frameworks. Heightened board-level oversight of cyber resilience, operational risk, and data governance further reinforced the sector's mission-critical positioning, sustaining strong investor and strategic acquirer interest.

Strategic buyers and financial sponsors targeted cybersecurity and GRC providers operating at the center of enterprise risk ecosystems, viewing control of security architecture, compliance workflows, and regulatory oversight as foundational to durable platform value. Acquisition strategies emphasized scaling managed security capabilities, expanding regulatory certification and audit services, increasing penetration within regulated industries, and integrating technology-enabled monitoring and analytics solutions. Buyers prioritized businesses with recurring revenue, high customer retention, technical specialization, and deep integration into enterprise governance and compliance operations.

This report analyzes M&A activity and valuation dynamics across the sector, including capital deployment trends, geographic investment patterns, acquirer composition, and valuation benchmarks. The analysis highlights continued consolidation, platform formation, and the growing strategic importance of scalable, compliance-driven cybersecurity services embedded within modern enterprise risk infrastructure.

EXHIBIT 1

Structural Growth Drivers Supporting Cybersecurity and GRC Services M&A

- **Escalating Cyber Threat Environment:** Persistent ransomware activity, supply chain vulnerabilities, and critical infrastructure exposure continue to elevate cybersecurity to a board-level priority. Organizations increasingly require ongoing risk monitoring, incident response readiness, and compliance oversight embedded within enterprise operations.
- **Expanding Regulatory and Compliance Mandates:** Governments and regulatory bodies are introducing increasingly stringent requirements across data protection, cyber resilience, financial reporting controls, and operational governance. This drives sustained demand for audit, certification, advisory, and managed compliance services.
- **Digital Transformation and AI Adoption:** Cloud migration, digital platform expansion, and AI deployment are increasing enterprise complexity and risk exposure. As digital ecosystems scale, governance frameworks and security controls must evolve accordingly, reinforcing structural demand for GRC capabilities.
- **Shift Toward Recurring Managed Service Models:** Clients are transitioning from project-based advisory engagements to recurring managed security, compliance monitoring, and outsourced risk functions, enhancing revenue visibility and platform attractiveness for acquirers.

Source: Global Research global consulting market outlook; McKinsey & Company 2026 M&A Trends report; McGladrey Quarterly Private Equity Deal Flow Profile; industry cybersecurity and governance market commentary.



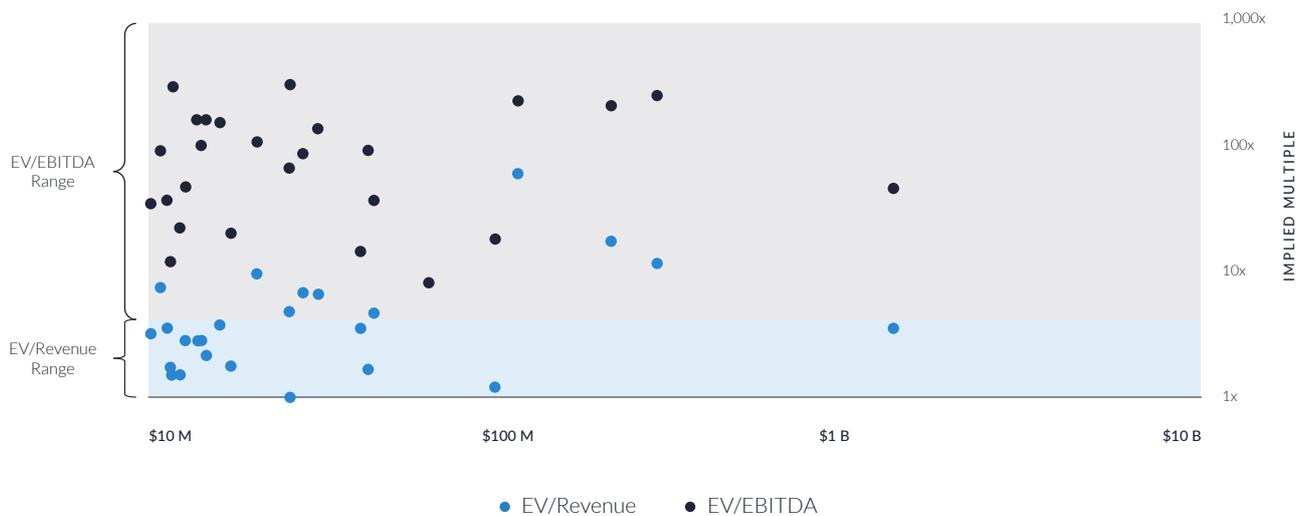
EXHIBIT 2

Consolidation and Investment Themes Shaping Cybersecurity and GRC Services Sector

- Fragmented Market Driving Platform Formation:** The sector remains highly fragmented across advisory, certification, and managed security providers, creating sustained roll-up opportunities for private equity sponsors and strategic acquirers.
- Technology-Enabled Services Convergence:** Firms are increasingly integrating proprietary GRC software, automation tools, and AI-enabled analytics into traditional advisory services, improving scalability, differentiation, and margin profile.
- Cross-Border and Sector-Specific Expansion:** Buyers are targeting geographic expansion and regulated vertical specialization (e.g., financial services, healthcare, critical infrastructure) to strengthen competitive positioning and diversify revenue streams.
- Capability-Led M&A Prioritization:** Acquirers are focusing on differentiated expertise, recurring revenue models, and embedded client relationships as key drivers of transaction activity and valuation resilience.

Source: Global Research consulting market analysis; McKinsey & Company 2026 M&A Trends report; McGladrey Quarterly Private Equity Deal Flow Profile; industry cybersecurity and compliance market analysis.

Transaction Valuation Multiples in the Cybersecurity, Governance, Risk and Compliance Services Sector Analysis (Q1 2021 – Q4 2025)



Axes are presented on a logarithmic scale to improve visualization of valuation dispersion.

EV / REVENUE

MEAN

5 X

MEDIAN

3 X

MINIMUM

1 X

MAXIMUM

65 X

EV / EBITDA

MEAN

83 X

MEDIAN

48 X

MINIMUM

1 X

MAXIMUM

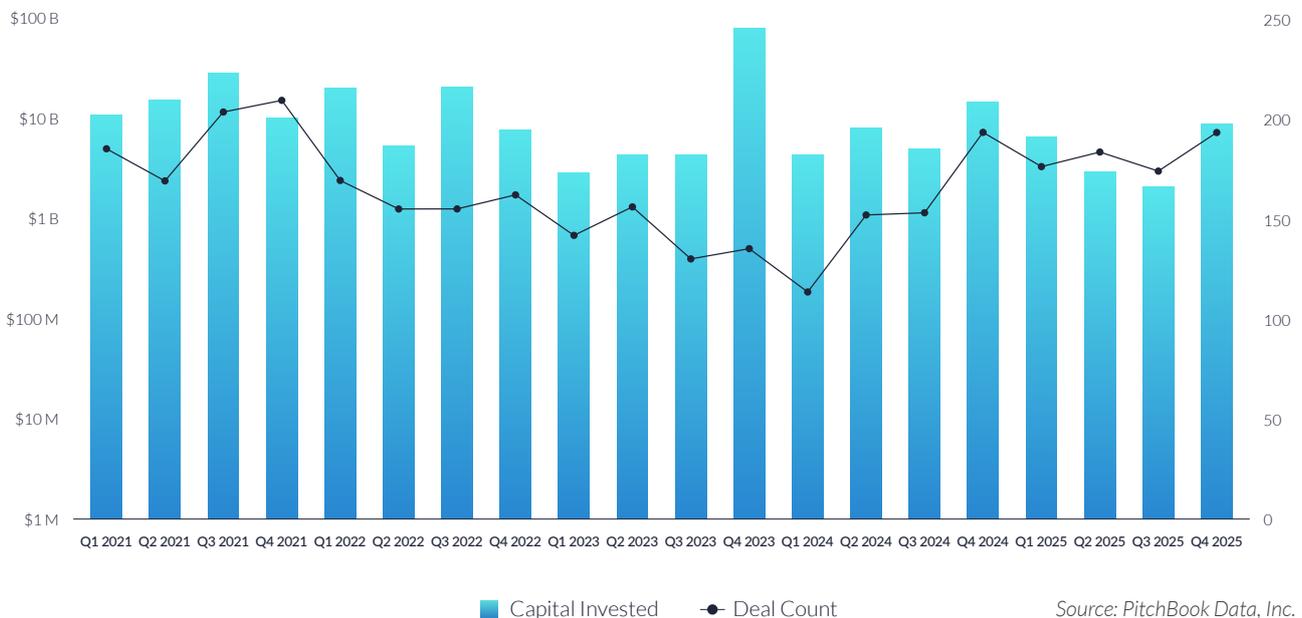
341 X

- Valuation multiples are based on a sample set of M&A transactions in the cybersecurity, governance, risk and compliance services sector using data collected as of February 18, 2026.
- EV/revenue multiples range from 1x to 65x, while EV/EBITDA spans 1x to 341x, reflecting significant dispersion driven by differences in revenue visibility, margin profile, growth trajectory, and strategic positioning. Assets commanding double-digit revenue multiples are likely recurring, software-embedded, or mission-critical cybersecurity platforms, whereas lower-multiple transactions (1x–4x revenue) skew toward services-heavy, labor-intensive compliance and consulting businesses. The wide EBITDA range further underscores inconsistent profitability across targets, with premium valuations concentrated among scalable, higher-margin platforms.
- Several large enterprise value transactions priced at materially higher revenue multiples relative to the broader dataset median (largely clustered between 1x–4x). This indicates strong strategic and sponsor demand for scaled cybersecurity and GRC platforms with enterprise penetration, embedded customer relationships, and durable recurring revenue. Larger platform assets appear to benefit from scarcity value and consolidation optionality, supporting multiple expansion relative to smaller tuck-in acquisitions.
- Despite headline outliers, the dataset shows a meaningful concentration of deals between 1x–3x EV/revenue, suggesting that much of the core cybersecurity and compliance services ecosystem continues to trade on traditional professional services metrics. This reflects margin sensitivity, talent dependency, and lower operating leverage compared to software-centric security models. The valuation bifurcation between high-growth, technology-enabled platforms and traditional advisory or compliance providers remains a defining characteristic of the sector.

CAPITAL MARKETS ACTIVITIES

The data highlights transaction activity, capital deployment, valuation dispersion, and geographic trends within the sector. Escalating cyber threats, expanding regulatory mandates, and increasing enterprise digital exposure continue to drive sustained M&A across managed security, compliance advisory, risk management, and governance service providers. Acquirers increasingly target scaled, security-critical platforms embedded within enterprise risk and IT infrastructure environments, prioritizing businesses with recurring revenue characteristics, strong client retention, and differentiated capabilities across monitoring, assessment, remediation, and regulatory compliance functions.

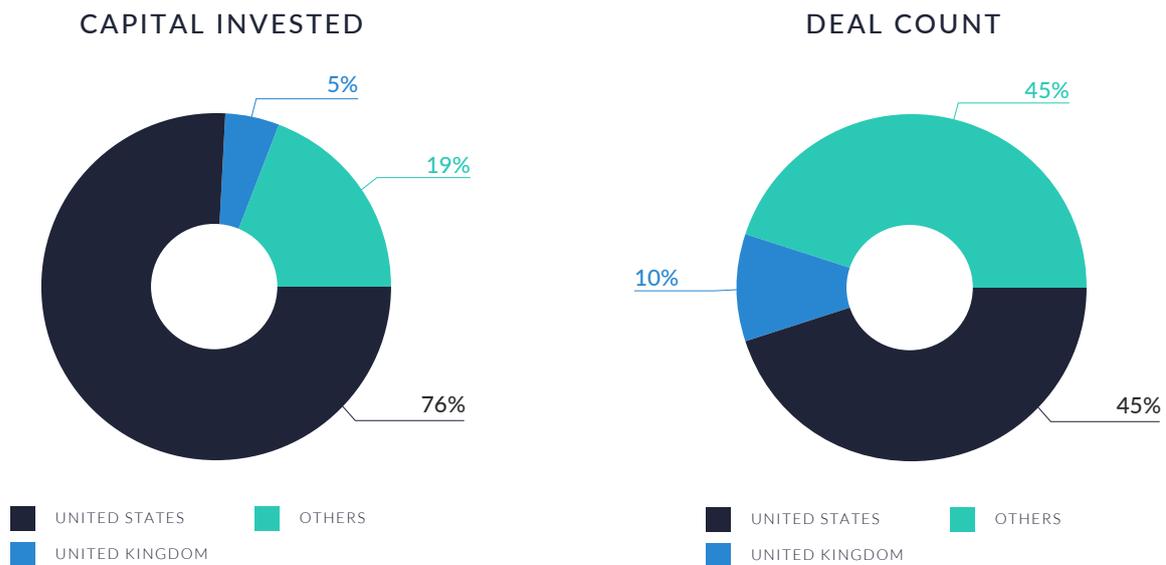
Announced M&A Transactions in the Cybersecurity, Governance, Risk and Compliance Services Sector (Q1 2021 – Q4 2025)



- Over the 20-quarter period, the sector recorded approximately \$253 billion of total capital invested across 3,308 transactions, underscoring sustained strategic and financial sponsor interest. The consistent transaction volume reinforces the sector's positioning as a core, non-discretionary investment theme driven by regulatory complexity, rising digital risk exposure, and ongoing enterprise security modernization.
- While quarterly capital invested fluctuated materially, deal count remained relatively stable, generally ranging between 130–200 transactions per quarter. This stability indicates continued middle-market consolidation and sponsor activity even during tighter capital markets, with investors emphasizing add-ons and smaller platform expansions.

- Capital deployment was uneven, with pronounced spikes in Q3 2021 (\$28 billion) and particularly Q4 2023 (\$77 billion), suggesting the impact of large-scale strategic or take-private transactions. Excluding these outlier quarters, capital deployment trends normalize to approximately \$2 billion–\$15 billion per quarter, reflecting steady but disciplined investment activity.
- Following a capital slowdown through much of 2023, the sector demonstrated renewed momentum in Q4 2024 (\$14 billion) and maintained healthy deal activity throughout 2025, with transaction counts exceeding 170 deals in most quarters. This pattern signals improving sponsor confidence, valuation normalization, and continued consolidation within the fragmented cybersecurity and GRC services landscape.

Breakdown of Announced M&A Transactions in the Cybersecurity, Governance, Risk and Compliance Services Sector by Country (Q1 2021 – Q4 2025)

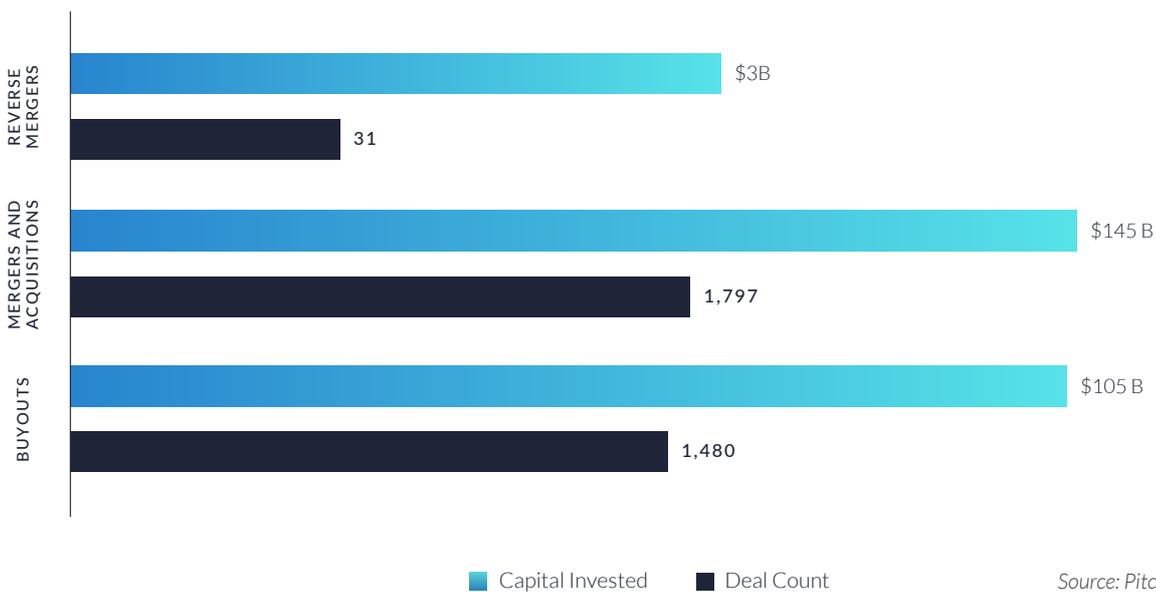


- The United States accounts for 76% of total capital invested while representing 45% of deal count, indicating that US-based investors execute disproportionately larger, platform-scale transactions. Deep private equity capital pools, mature cybersecurity demand, and a high concentration of

regulated enterprises enable US buyers to pursue valuation-setting acquisitions. As a result, US capital materially influences consolidation strategies, competitive dynamics, and pricing benchmarks across the global cybersecurity and GRC landscape.

- International and emerging markets represent 45% of deal count but only 19% of capital invested, reflecting frequent yet smaller-scale transactions. Buyers in these regions typically pursue add-on acquisitions and mid-market consolidation strategies, consistent with more fragmented, services-oriented business models. Nevertheless, rising global regulatory standards and increasing cyber risk exposure continue to sustain international deal flow, positioning these markets as strategically important growth and expansion arenas despite lower average deal sizes.
- The United Kingdom accounts for 10% of deal count and 5% of capital invested, signaling consistent transaction activity at moderate scale. Strong financial services exposure, regulatory rigor, and established governance frameworks support steady M&A activity. However, the comparatively lower capital concentration suggests a predominance of mid-market transactions rather than large-scale platform buyouts.

Breakdown of Announced M&A in the Cybersecurity, Governance, Risk and Compliance Services Sector by Deal Type (Q1 2021 – Q4 2025)



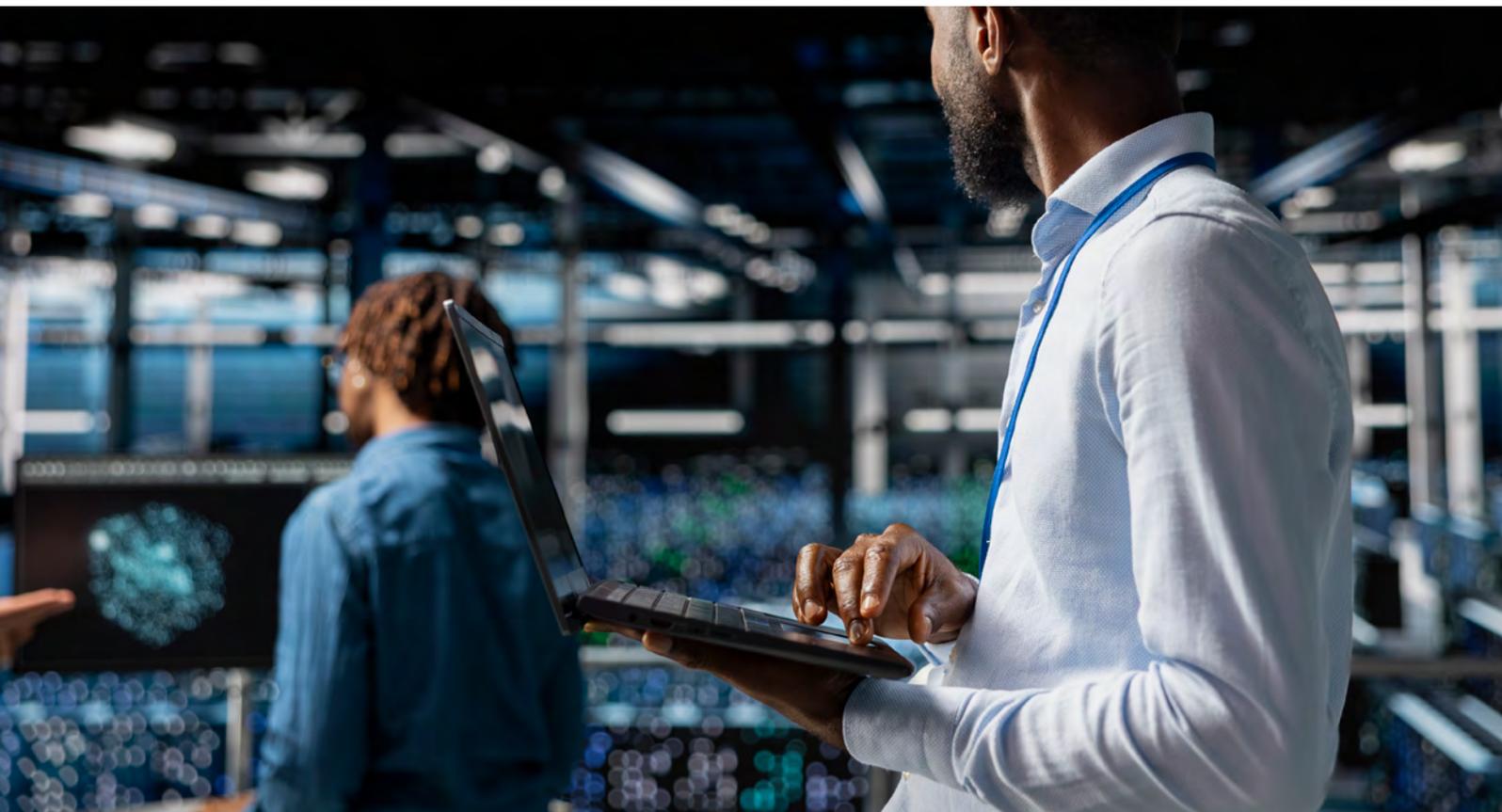
- Mergers and acquisitions accounted for \$145 billion across 1,797 transactions, representing the largest share of both capital deployed and deal volume. This underscores significant strategic buyer participation, with corporates actively consolidating capabilities, broadening service offerings, and strengthening regulatory and security expertise through bolt-on acquisitions and platform expansion.

- Buyouts totaled \$105 billion across 1,480 transactions, highlighting sustained private equity conviction in the cybersecurity and GRC sector. The substantial activity reflects ongoing platform formation and add-on strategies, particularly within fragmented compliance, managed security, and advisory segments.
- Reverse mergers were limited, totaling \$3 billion across 31 transactions, indicating that public market access via alternative listing structures has not been a primary capital strategy for the sector. Instead, private-to-private transactions and sponsor-backed deals remain the dominant mechanisms for growth and liquidity.
- The relatively balanced distribution between strategic M&A and buyout activity reflects a competitive and well-capitalized buyer universe. The presence of both corporates and financial sponsors likely supports sustained transaction volume and competitive valuation dynamics, particularly for scaled, differentiated cybersecurity platforms.



M&A TRANSACTIONS CASE STUDIES

Three transactions in the sector illustrate how investors are scaling services-led platforms embedded within enterprise security and regulatory frameworks. Acquirers are targeting firms that provide cybersecurity advisory, payment card industry compliance, and risk management services designed to address escalating cyber threats and expanding regulatory obligations. These transactions reflect strong demand for compliance-driven platforms characterized by recurring revenue, high customer retention, and deep integration into enterprise risk management functions, positioning governance, risk, and compliance providers as mission-critical partners within modern security infrastructure.



CASE STUDY 01

COALFIRE

C O A L F I R E .

Coalfire Systems, Inc. is a US -based cybersecurity advisory and assessment services firm specializing in compliance, risk management, and cloud security. The company provides Payment Card Industry Data Security Standard assessments, regulatory compliance audits, cybersecurity testing, and advisory services to enterprises, financial institutions, government agencies, and cloud-native organizations. Coalfire operates as a Qualified Security Assessor and supports clients in meeting complex regulatory requirements while strengthening overall security posture. Its service offerings are embedded within enterprise risk and compliance frameworks, generating recurring advisory and assessment revenue through long-term customer relationships.

TRANSACTION TYPE

BUYOUT

DEAL DATE

APRIL 22, 2020

ACQUIRER

APAX PARTNERS

ENTERPRISE VALUE

\$350 MILLION

ACQUIRER

Apax Partners is a global private equity firm with significant experience investing in technology, services, and internet platforms. The firm focuses on partnering with market-leading companies that demonstrate scalable business models, strong cash flow visibility, and opportunities for operational and strategic value creation. Apax has an established track record in cybersecurity and technology-enabled services investments.

TRANSACTION STRUCTURE

Coalfire was acquired by Apax Partners through a leveraged buyout transaction valued at approximately \$350 million, completed on April 22, 2020.

MARKET AND CUSTOMER SEGMENTS COMBINATION

The transaction combined Apax Partners’ experience scaling technology-enabled services businesses with Coalfire’s established cybersecurity and compliance advisory platform. Under private equity ownership, Coalfire continued to serve enterprise clients across financial services, healthcare, government, and cloud-focused industries requiring mission-critical compliance certifications and security validation. The investment provided additional strategic and financial resources to expand service offerings, deepen penetration within regulated industries, and accelerate growth in cloud security and compliance services.

ACQUISITION STRATEGIC RATIONALE

The acquisition reflected sustained private equity demand for cybersecurity and compliance platforms benefiting from regulatory tailwinds, recurring client engagements, and high switching costs driven by audit relationships and industry certifications. Coalfire’s position as a trusted assessor and advisor within regulated environments, combined with predictable assessment revenue and expanding demand for cloud security services, positioned the company as an attractive platform for continued investment and operational scaling. The transaction aligned with Apax Partners’ strategy of investing in scalable, compliance-driven technology services businesses characterized by durable demand and long-term growth visibility.

KEY INTANGIBLE ASSETS



Qualified Security Assessor Status



Trusted Audit Relationships



Regulatory Brand Credibility

TRANSACTION RATIONALE



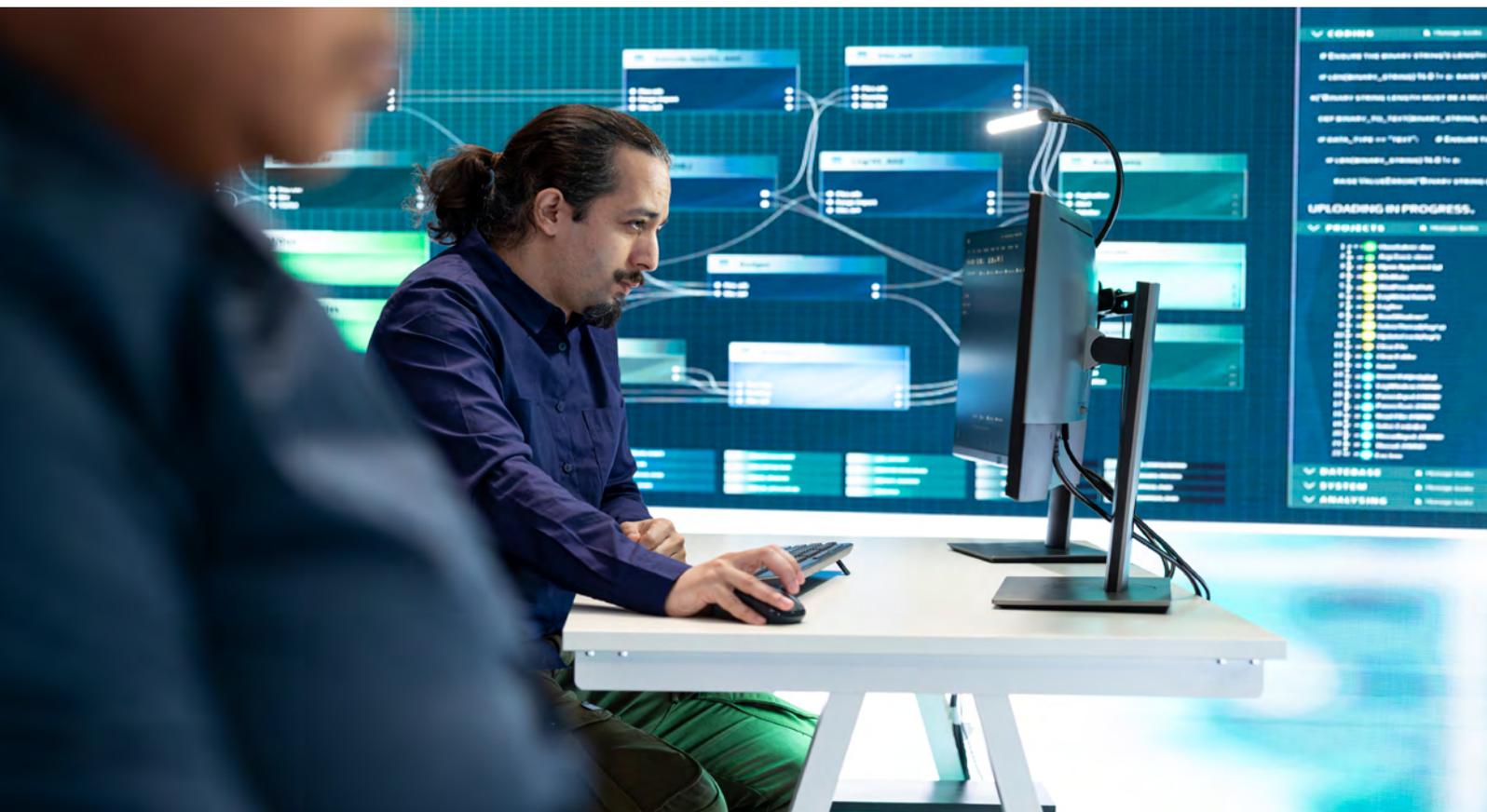
Regulatory Demand Growth



Assessment Platform Scale



Cloud Security Expansion



CASE STUDY 02

OPTIV SECURITY



Optiv Security, Inc. is a United States-based cybersecurity solutions and services provider delivering end-to-end security advisory, managed security services, risk management, cloud security, and compliance solutions to enterprise and mid-market organizations. The company supports clients across financial services, healthcare, government, and technology sectors with cybersecurity strategy, threat detection, vulnerability management, identity governance, and regulatory compliance, including Payment Card Industry Data Security Standard assessments. Optiv's services are embedded within clients' enterprise security architectures, generating recurring revenue through long-term advisory engagements, managed services contracts, and ongoing compliance support.

TRANSACTION TYPE

BUYOUT

DEAL DATE

JANUARY 26, 2017

ACQUIRER

KOHLBERG KRAVIS ROBERTS

ENTERPRISE VALUE

\$2 BILLION

ACQUIRER

KKR is a global investment firm specializing in private equity, credit, and alternative asset management, with significant experience investing in technology-enabled services and cybersecurity platforms. The firm focuses on partnering with scaled businesses that demonstrate strong growth potential, durable client relationships, and opportunities for operational and strategic value creation through capital investment and platform expansion.

TRANSACTION STRUCTURE

Optiv Security was acquired by KKR through a majority-stake leveraged buyout transaction that was announced in December 2016 and completed in early 2017, for approximately \$2 billion.

MARKET AND CUSTOMER SEGMENTS COMBINATION

The transaction combined KKR’s experience scaling technology-enabled services businesses with Optiv’s established cybersecurity advisory and managed services platform serving enterprise clients. Under private equity ownership, Optiv continued to support organizations requiring integrated cybersecurity strategy, compliance, and managed detection services. The investment provided additional capital and strategic resources to expand service capabilities, pursue acquisitions, enhance managed security offerings, and deepen penetration across regulated and enterprise end markets.

ACQUISITION STRATEGIC RATIONALE

The acquisition reflected strong private equity interest in cybersecurity platforms benefiting from structural demand drivers, including rising regulatory requirements, increasing cyber threats, and growing enterprise reliance on outsourced security expertise. Optiv’s recurring managed services revenue, compliance-driven engagements, and mission-critical role within client security frameworks positioned the company as an attractive platform for long-term investment. The transaction aligned with KKR’s strategy of investing in scalable, services-based technology businesses with predictable revenue streams, high customer retention, and opportunities for operational enhancement and strategic growth.

KEY INTANGIBLE ASSETS



Enterprise Client Relationships



Broad Partner Ecosystem



Established Security Solutions Brand



Global Expansion Enablement

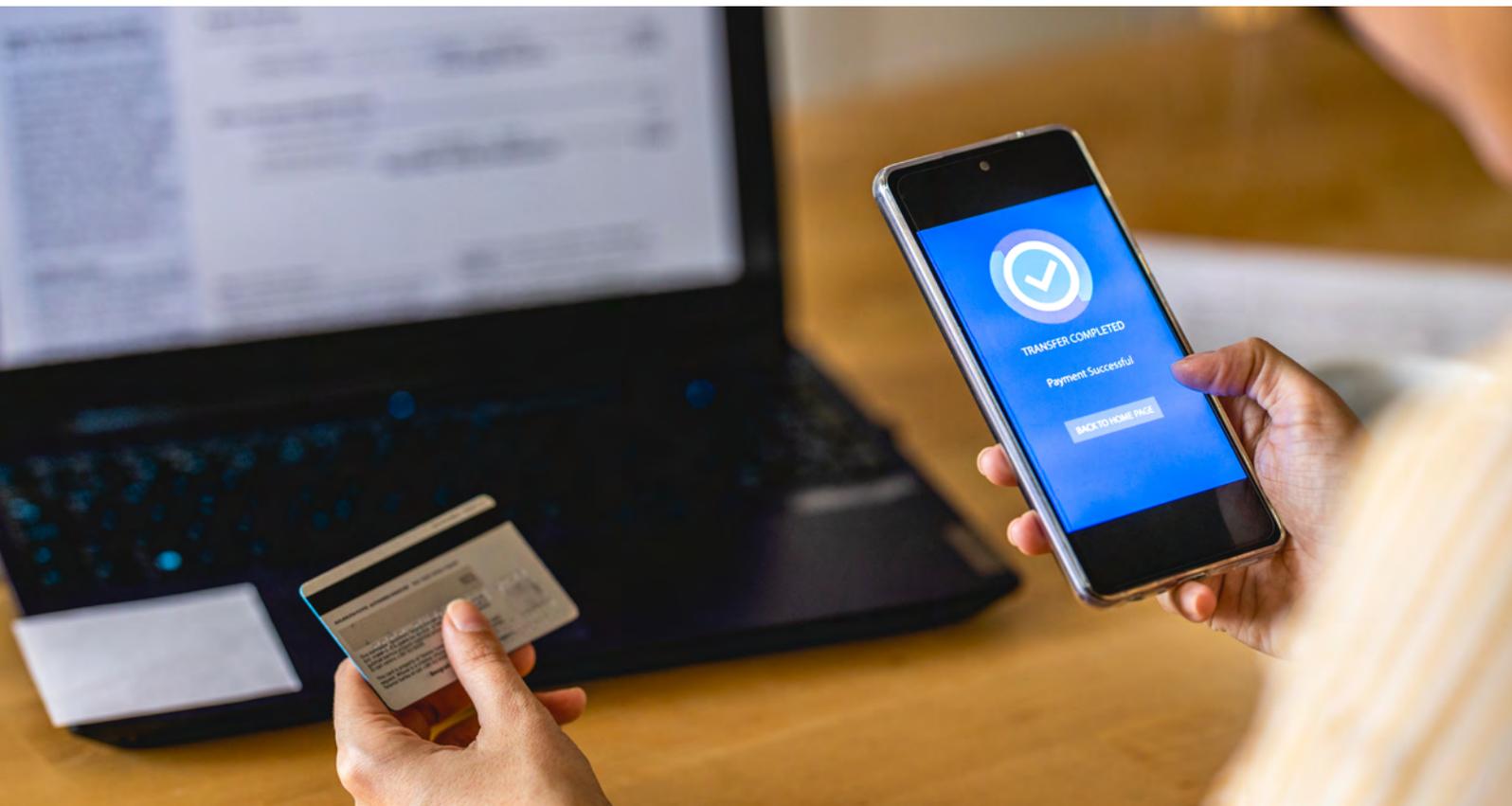


Managed Security Services Scale



Recurring Compliance Revenue

TRANSACTION RATIONALE



CASE STUDY 03 PAYMENT SOFTWARE COMPANY



Payment Software Company, Inc. was a United States-based cybersecurity and compliance consulting firm specializing in payment security, Payment Card Industry Data Security Standard assessments, and secure payment application validation. The company provided advisory, audit, and certification services to merchants, service providers, and payment technology companies seeking compliance with cardholder data security standards. As a Qualified Security Assessor and Payment Application Qualified Security Assessor, Payment Software Company supported clients in navigating complex regulatory requirements and maintaining ongoing compliance. The company generated revenue through assessment engagements, consulting services, and recurring compliance advisory relationships.

TRANSACTION TYPE

M&A

DEAL DATE

SEPTEMBER 29, 2016

ACQUIRER

NCC GROUP (LON: NCC)

ENTERPRISE VALUE

\$19 MILLION

ACQUIRER

NCC Group plc is a United Kingdom-based global cybersecurity and software resilience company providing assurance, advisory, testing, and compliance services to enterprises, governments, and financial institutions. The firm has pursued a strategy of expanding its services-led cybersecurity capabilities across Europe and North America through targeted acquisitions that strengthen technical expertise and geographic presence.

TRANSACTION STRUCTURE

Payment Software Company was acquired by NCC Group on September 29, 2016, for total consideration of approximately \$19 million.

MARKET AND CUSTOMER SEGMENTS COMBINATION

The acquisition combined NCC Group’s global cybersecurity and assurance platform with Payment Software Company’s established payment security and Payment Card Industry Data Security Standard compliance expertise in the United States. Payment Software Company’s specialization in card payment security assessments complemented NCC Group’s broader risk management, penetration testing, and software escrow services. The transaction strengthened NCC Group’s presence in the North American market and enhanced its ability to serve financial institutions, payment processors, and regulated enterprises requiring Payment Card Industry validation and compliance advisory services.

ACQUISITION STRATEGIC RATIONALE

The acquisition aligned with NCC Group’s strategy of acquiring services-led cybersecurity businesses to expand both geographic footprint and technical capabilities. Payment Software Company’s reputation in payment security and Payment Card Industry compliance added specialized expertise in a highly regulated segment characterized by recurring audit demand and strong customer retention. The transaction positioned NCC Group to deepen its penetration within the global payments ecosystem and capitalize on expanding regulatory and cybersecurity requirements across enterprise and financial services clients.

KEY INTANGIBLE ASSETS



Qualified Security Assessor Accreditation



Payment Application Assessment Expertise



Established Payment Industry Relationships

TRANSACTION RATIONALE



North American Market Expansion



Payment Security Capability Enhancement



Recurring Audit Revenue Growth

As enterprise risk management becomes increasingly embedded within digital infrastructure, cybersecurity and governance, risk, and compliance services have evolved from specialized advisory functions into core components of operational resilience and regulatory oversight. Sustained transaction activity over the past five years reflects investor conviction that security- and compliance-driven platforms embedded within enterprise information technology and risk workflows represent a durable, long-term asset class rather than a cyclical services theme.

Looking ahead, acquirers are expected to remain disciplined, prioritizing scaled platforms characterized by recurring revenue, technical specialization, and deep integration into client security architectures and compliance frameworks. Valuation dispersion is likely to persist, with premium outcomes concentrated among technology-enabled and managed services platforms, while continued consolidation among smaller advisory-led providers supports ongoing roll-up and platform formation strategies. As cyber threats intensify and regulatory scrutiny expands, well-integrated, execution-oriented platforms are positioned to anchor future consolidation and sustained value creation across the cybersecurity and governance, risk, and compliance services landscape.

SOURCES

APAX PARTNERS COMPLETES COALFIRE ACQUISITION -
PR NEWSWIRE



OPTIV SECURITY TO BE ACQUIRED BY PRIVATE EQUITY
FIRM KKR - SECURITY WEEK



KKR ACQUIRES OPTIV FOR \$1.9 BILLION - CHANNELE2E



NCC GROUP ACQUISITION OF US CYBER SECURITY AND
PAYMENT CONSULTANCY FOR UP TO \$18.75M - BABC



PITCHBOOK DATA



JAHANI & ASSOCIATES

Jahani and Associates (J&A) is a global investment bank headquartered in New York City. J&A has deep connections in the Middle East, Southeast Asia, Latin America, and North America. The firm provides investment banking advisory, investment banking transaction, and corporate development expertise to clients all over the world.

641 Lexington Ave 15th floor, New York, NY 10022

+1 (646) 851 0654 | +971 04 230 6084 | +65 6622 5421

info@jahaniandassociates.com | jahaniandassociates.com

The opinions and views expressed in this report may not necessarily reflect the institutional views of J&A or its affiliates. This report should not be copied, distributed, reproduced, or published in whole or in part or disclosed by any recipient to any other person without the express written consent of Jahani and Associates. Each name of the third-party organization or organizations mentioned in this report is the property of the company to which it relates. It is used here strictly for informal identification purposes only and is not used to imply any ownership or license rights between any such company and J&A. The content of this program does not constitute a recommendation from any J&A entity to the recipient and is provided for informational purposes only. J&A is not providing any financial, economic, legal, investment, accounting, or tax advice through this report or to its recipient. Certain information in this report contains forward-looking statements and there is no guarantee that these results will be achieved. J&A has no obligation to provide updates or changes to the information in this report. Past performance does not guarantee future results, which may vary. Neither J&A nor any of its affiliates make any representation or warranty, expressed or implied, as to the accuracy or completeness of the statements in this report or any information contained in this report, and any liability therefore, including, and in respect of direct and indirect consequential loss or damage, is expressly disclaimed.