BRG

INTELLIGENCE THAT WORKS

BRAD WILSON

BERKELEY RESEARCH GROUP (BRG), LLC
70 W Madison, Suite 5000 | Chicago, IL 60602
Direct: 312.253.3496
bwilson@thinkbrg.com

SUMMARY

Brad Wilson is a managing director in BRG's Economics, Disputes & Investigations practice and specializes in cybersecurity, AI audits and investigations, as well as AI governance, risk and compliance. His experience includes cybersecurity risk and AI assessments, national security advisor, The Committee on Foreign Investment in the United States (CFIUS) audits and monitorships, insider threats, data analytics, and eDiscovery in the healthcare, technology, pharmaceutical, finance, communications, industrial, and government sectors. His advisement has led to business improvements—and inherent competitive advantages—through risk mitigation and digital transformations. He also advises clients on managing AI and cyber risk through assessments of supply chains, enterprise architectures, data-driven analytics, and integrating program management into complex corporate structures.

Mr. Wilson has conducted a number of investigations into unauthorized use of Generative AI and third-party tools. He advises clients on national security compliance issues and process control improvements involving sensitive data identification, vendor management, and identity access management. He has served as the CFIUS-approved auditor for AI-focused audits, responsible for evaluating compliance with data protection, AI integrations, and physical/logical access control requirements related to customer information and log data. For a multinational financial company, Mr. Wilson supervised a cybersecurity investigation of suspicious wire fraud transfers with allegations of insider and external threat actors; and managed the business email compromise investigation that included fact-finding and analysis of financial and digital artifacts. He has also led cybersecurity investigations stemming from theft of trade secrets, network intrusions, and diversion of funds for clients in the banking, medical device, and construction sectors; and corporate investigations related to allegations ranging from fraud, antitrust, and other serious crimes.

Mr. Wilson focuses on integrating technological approaches, including machine learning (ML) and artificial intelligence (AI), to drive insights and make informed decisions. He has applied predictive analytics to disparate data sources to react to trends before they become risks. Before he joined BRG, he assisted compliance, legal, and internal audit teams to align policies and procedures to address these business risks. He assists clients in achieving greater business value through digital transformations of their compliance programs. In one case, to quickly close critical gaps in a compliance process, he performed a rapid digital transformation of the company's compliance program to avoid risks and save cost. These efforts led to a corporate compliance program focused on resilience and continuous improvement.

Mr. Wilson previously was a director in the Cybersecurity, Privacy, and Forensics practice for a Big Four advisory firm, where he was influential in driving innovation in discovery solutions, ML, AI, legal operations, and performance improvement. He has extensive experience building and implementing discovery, data-security readiness programs, and other incident-response programs through data handling, data mapping, policies and procedures, education, and awareness programs. He also has advised on legal operations relating to strategic assessments, prioritization, and implementation of process improvements, while enhancing and streamlining a company's core functions.

AI Governance Risk and Compliance

- A U.S.-based data services company was acquired by a Japanese investment holding company in a CFIUS-reviewed traction. Mr. Wilson served as the CFIUS-approved auditor responsible for evaluating compliance with data protection and physical and logical access control requirements relating to customer information and log data. The audit included focused review of new internal and customer-facing deployments of third-party artificial intelligence tools, identifying a compliance violation and risks of unauthorized access pathways to sensitive data caused by the AI integrations. The assessment included technical configurations, access logs, and controls to evaluate compliance with CFIUS requirements and provided recommendations to support the secure implementation of emerging AI technologies within the company's operational environment.
- A global communications firm sought to embrace artificial intelligence but needed to comply with stringent CFIUS compliance obligations to turn the CEO's ambitious vision into a tangible plan. Mr. Wilson helped ensure CFIUS compliance obligations were met for both immediate needs and comply with long-term, self-sufficient capabilities. This included evaluations of policies, risk management framework (RMF) based on the NIST AI RMF and ISO 42001, and technical AI compliance controls. Mr. Wilson also provided technical assessments of infrastructure and AI technology being developed by the product and engineering team to assess and mitigate CFIUS compliance obligations involving their domestic communications infrastructure and principal equipment, document change over time and improve audit readiness.
- A professional services company identified potential misuse of generative AI tools following concerns about unauthorized development activity and handling of confidential information. An employee independently developed an AI-enabled workflow to accelerate RFP creation after viewing a demonstration of a third-party SaaS platform. The workflow was built using frontier models accessed through a third-party development environment, without company approval, and incorporated confidential company information and sensitive client data. The activity occurred outside of established governance, security, and approval processes. Mr. Wilson supported the client in investigating the scope of AI usage, data exposure, and third-party processing risks. This included assessing whether confidential materials were used to train or interact with external models, supporting the removal of source documents, and evaluating compliance with internal policies and contractual obligations.
- A cybersecurity investigation of a company in the generative AI and cloud compute/infrastructure industry. The allegations involved improper AI image-generation content and related compliance and reputational risk. Mr Wilson assessed the AI company's technical and contractual control environment (including terms of service and user restrictions), evaluated existing and planned AI guardrails (e.g., content captioning, age-detection tooling, reporting mechanisms, and audit concepts), and advised on investigative and evidence-preservation steps to responsibly identify and segregate potentially unlawful content. He also helped frame decision-ready options for leadership, including guidance regarding thresholds and timing considerations for external reporting obligations and the internal control enhancements needed to monitor and manage use of underlying AI compute infrastructure.

Cybersecurity Expertise

- On behalf of a global financial services company, conducted a cybersecurity maturity assessment across the protect, detect, respond, educate, and govern cyber domains. Leveraging a quantitative scoring system based on the NIST Cybersecurity Framework 2.0, assessed the company's cybersecurity posture with a rating from one (critical weaknesses) to five (optimized resilience), evaluating both overall risk management and the effectiveness of Confidentiality, Integrity, and Availability (CIA) controls. The methodology combined analysis of key documentation, observation of operational practices, and interviews with personnel across 22 cyber domains, providing a clear, data-driven view of current strengths and areas for improvement. The assessment highlighted present maturity and identified opportunities to enhance the company's overall resilience against cyber threats.
- On behalf of a multinational energy company, conducted a large-scale data leakage response involve multiple global jurisdictions. Through hundreds of scoping interviews, data mapping, and data sampling, quantified personally identifiable information and personal health information that had been improperly shared externally. Assessed cyber risks and analysis of disparate systems to quantify exposure and prepare the information for disclosures.
- Assisted external counsel and corporate leadership of a financial technology services company with a large-scale data breach investigation of payment card information. Throughout the investigation, led the digital forensic collections of endpoint, enterprise and network information, and subsequent analysis using big data technology to analyze billions of forensic artifact records. Consolidated findings into visual link analysis reports and quantified exposure for reporting to government agencies and law firms.
- On behalf of a financial services company with global operations, assisted with a business email compromise (BEC) investigation that involved spear phishing and wire transfer fraud totaling over $20 million. Provided internal investigative expertise to assist internal fraud team to understand the timeline of events, generate investigative report outlining the facts, generate cyber intelligence on threat actors, and provide digital forensic expertise. The report and findings were used to inform affected customers on key events and apply lessons learned to improve fraud detection and employee awareness training.
- On a similar matter for a company providing healthcare services, provided digital forensic expertise with a BEC investigation involving social engineering and wire transfer fraud totaling over $50 million. Provided investigative expertise to internal and external general counsel on the parties of interest involved, interview support, digital forensic collection of enterprise, and endpoint devices to determine internal versus external threat vector. Extensive analysis of endpoint and mobile devices to understand timeline and location information.
- Implemented cybersecurity program management and network security monitoring appliance and investigative workflows for a retained company. Assisted general counsel and IT security teams with cybersecurity advisory expertise to improve their security posture with deployment of enterprise network monitoring of external and internal cyber threats, building and implementing forensically sound data handling procedures, data mapping, policies and procedures, education, and awareness program.
- On behalf of a healthcare company, assisted with a trade secret fraud that involved proactive network communication and activity monitoring of employees to understand if sensitive company documents were being leaked to external parties. Implemented technology to monitor

communications and user activity on endpoint devices, recurring analysis of alerts and logs, and augmented internal investigative team to determine activity of interest.

- On a similar matter for a financial services company, assisted the chief information risk officer, insider threat director, and external counsel with intellectual property (IP) theft investigation of sensitive company information by an employee leaving the company. Forensically preserved and analyzed mobile, laptop, and network logs to determine sensitive information that had been sent to personal accounts. Assisted counsel with interview, classification, and quantification of information that was used during litigation with defense counsel.

Compliance, Forensic, and Data Analytics Expertise

- A US-based global telecommunications company required assistance in developing policies and procedures to effectively meet US national security requirements around protecting sensitive information from foreign exploitation. Services consisted of developing a detailed security plan that included novel logical and physical access restrictions, vendor management guidelines, integration restrictions, remote work restrictions, and training requirements. Additionally, provided a gap assessment of over fifty corporate policies, including all policies related to security and cybersecurity, to better align the policies with National Security Agreement (NSA) requirements; provided discovery and cyber-risk management services across numerous lines of business to help the company identify locations of its CFIUS-defined sensitive assets; assisted in determining who in the company's global workforce had access to those sensitive assets; and provided recommendations on supply chain and vendor management improvements.
- For a multinational medical device manufacturer, assisted general counsel and external counsel to quantify the impact of medical devices gathering large amounts of sensitive personal and health information for diagnostic and maintenance purposes. Assisted with data mappings of information flows, forensic collection of disparate systems including QuickBooks, data analytics for quantification, and third-party disclosure reporting.
- For a global healthcare provider, assisted compliance, general counsel, and internal audit teams to align policies and procedures to address business risks. Used AI/ML to aggregate and identify common themes within large amounts of hotline intake systems. Combined the structured and unstructured data sources to initiate investigative review workflows and generate weekly insight reports for company executives.
- For a large manufacturing company and external counsel, provided business improvements—and inherit competitive advantages—through automations and digital transformations in responding to an Environmental Protection Agency (EPA) investigation. Support required forensic preservation and extraction of documents and information from the company's Zoho customer relationship management (CRM) system, analysis of metadata, and presentation of findings. Supported regulatory compliance program technical improvements in identifying gaps, process improvement recommendations, and implementations through their Zoho CRM system. Assisted with compliance program improvements within the CRM platform to facilitate vendor management, document retention, digital workflows, and automations to both improve EPA compliance and inherit business improvements.
- On behalf of a multinational pharmaceutical manufacturing company, conducted a large-scale product liability and mass tort response involving multiple global jurisdictions. Assisted external counsel team globally with collection and review of disparate custodial and enterprise data

sources both across Asia and in the European Union. Implemented globally consistent methodology and streamlined document review with over 20 million records.

- Assisted special committee and external counsel of a publicly traded consumer products company in conducting an internal investigation and Securities and Exchange Commission (SEC) and Department of Justice (DOJ) investigations into potential Foreign Corrupt Practice Act (FCPA) violations in China. During early stages of investigation, provided digital forensic expertise on user behavior and deletion trends, which helped drive insightful interviews and enabled streamlined review workflows.
- In a similar matter brought by the SEC and DOJ, provided investigative support involving allegations of anti-bribery and corruption for a Fortune 500 communications company. Supported company and counsel with forensic technology expertise with preservation, analysis, and review of company communications, documents, transactions, and supporting documentation with global assistance in the US, Brazil, and China. Led efforts to analyze and prepare forensic report on procedures performed, deletion analysis results, and responding to government requests with document productions.
- On behalf of a multinational biotechnology company, assisted external counsel with a regulatory inquiry relating to an antitrust matter. Coordinated global team across Switzerland, China, the Netherlands, and US with forensic collections of endpoint devices and enterprise technologies, including both Salesforce and Documentum.

National Security and Government Experience

- For a US technology company, provided policy and technical advisory services to help bring the company into compliance with its NSA. Services consisted of developing a detailed security plan that included novel logical and physical access restrictions, vendor management guidelines, integration restrictions, remote work restrictions, and training requirements. Additionally, provided a gap assessment of over fifty corporate policies to better align the policies with NSA requirements; provided discovery and cyber-risk management services across numerous lines of business to help the company identify locations of its CFIUS-defined sensitive assets; assisted in determining who in the company's global workforce had access to those sensitive assets; and provided recommendations on supply chain and vendor management improvements.
- For a US healthcare services company, served as the third-party monitor (TPM) for a transaction with a private-equity (PE) fund. Integrated necessary monitoring activities into the transaction parties with minimal impact on the business operations of both the US company and the PE fund. Particular emphasis was placed on communications between the company and the PE firm, including email, web-enabled conferences, and transaction data room, as well as logical and physical access requirements. Additionally, advised on current process and technology enhancements to meet weekly and monthly communication and access log review requirements.
- On behalf of the US Department of Treasury, assisted with Troubled Asset Relief Program (TARP) in providing program management assistance. Also provided expertise on implementing forensically sound procedures with Freedom of Information Act (FOIA) using industry-standard discovery workflows and documentation.
- On behalf of the Federal Deposit Insurance Corporation (FDIC), provided forensic collection and preservation expertise during the closing of bank assets. Adhered to forensically sound collection and documentation procedures.

EDUCATION

BS Pennsylvania State University, 2007

PRESENT EMPLOYMENT

Managing Director, BRG, 2024–present
Director, BRG, 2020–2024

PREVIOUS POSITIONS

PricewaterhouseCoopers (PWC), 2007–2020

CERTIFICATIONS

EnCase Certified Examiner (EnCE), Open Text Corporation 15-0709-3110
Certified Blacklight Examiner, Blackbag Technologies

PROFESSIONAL AFFILIATIONS

Present

Member, High Technology Crime Investigation Association
Member, USSS Chicago Electronic Crimes Task Force

BUSINESS AND NOT-FOR-PROFIT AFFILIATIONS

Advisory Board Member, St. John of the Cross School, Western Spring, IL

PUBLIC SPEAKING ENGAGEMENTS

Chicago U.S. Secret Service Cyber Fraud Task Force, Insider Threats and Shadow AI *(March 2026)*
ACI 12th National Conference on CFIUS, Analyzing CFIUS Reviews of Transactions in Critical Technology, AI and Quantum Computing Dual Use *(April 2026)*

PUBLICATIONS

ARTICLES

(1) "2021 NDAA: Securing Cyberspace Together" (with Eric Matrejek), *BRG*, 2021.

(2) "FCPA Investigations and "Private" Messaging Apps: What You Need to Know Now" (with Eric Matrejek), *American Bar Association*, 2018.