Karl V. Hopkins
Partner & Global Chief Security Officer

Partner & Global Chief Security Officer

Houston
D +1 713 658 4606

Washington, DC
D +1 202 408 9225

karl.hopkins@dentons.com

Overview

Karl V. Hopkins is a partner and Dentons' Global Chief Security Officer where he is responsible for managing the security for the world's largest law firm. Karl also chairs the Dentons Intelligence and Strategic Services Group, co-chairs the Global Security Risk Committee, serves on the Global Management Committee, and reports to the Global Board.

Karl counsels the Firm on international strategy, business and political intelligence, and security and threat analysis. In addition, he provides strategic advice to the Firm's clients regarding their global operations, including the performance of due diligence and compliance investigations, physical and cyber security assessments, country and political risk assessments, and threat analyses. This includes providing enterprise risk management and organizational resiliency advice.

Karl also provides clients with strategic and legal advice regarding crisis and incident response. He has managed various types of crises, including physical security breaches and cyber incidents, insider threats and reputational impacts. He also assists clients with the formulation and implementation of communication and crisis management policies and protocols. Karl is also known for his unconventional tabletop exercises, based entirely on real-life events, threat intelligence, and his client’s sectoral weaknesses.

Experience

Karl has represented clients on matters with touchpoints in over 50 countries.

- Represent a Fortune 100 energy company as its incident response counsel. Perform cybersecurity maturity and insider threat assessment.
- Provide counsel to a US Fortune 500 manufacturing company victimized by a business email compromise. Work with forensic teams to discover the breach’s root cause.
- Represent a global hotel chain against its vendor that suffered from a breach exposing credit card and PII of customers at over 32,000 hotels across 120 countries.

- Counsel a nation-wide retailer on the breach of consumer PII caused by the injection of keylogger malware.
- Advise a foreign financial institution in its response to the Equifax data breach for customer communications, contractual obligations, regulatory notifications, and indemnification claims.
- Design and play APT ransomware simulation tabletops for a Fortune 500 client. Perform vulnerability assessments; implement vertically and horizontally interacting multi-regional incident response teams operating on segmented communications platforms.
- Provide training based on a retail network attack simulation tabletop for a US-based client to assess its compliance with PCI DSS and FTC and CFPB regulatory framework.
- Simulate a supply-chain attack for a US-based industrial manufacturer based on Shadowpad and Kingslayer cyberattacks targeting cyber espionage on protected intellectual property.
- Develop an APT-attack monitoring policy for a US-based client built on indicators of threat analysis. Develop a simplified but comprehensive incident response plan based on various attack vectors.
- Provide counsel for pen-testing on a US-based smart-grid for compliance with the Homeland Security Guidelines on critical infrastructure.
- Create a risk analysis report for a US-based energy company assessing its zero-trust vulnerabilities. Recommend tailored SIEM technologies based on threat intelligence and geopolitical threat vectors analysis.
- Advise a foreign software developer on the impacts of the Federal Court’s 07/2020 ruling on the assertion of jurisdiction in WhatsApp Inc. v. NSO Grp. Techs., Ltd; analyze the Court's interpretation of the Computer Fraud and Abuse Act on activities involving NSO Grp.
- Provide counsel on the first CCPA settlement concerning violations for a failure to implement and maintain reasonable security procedures and practices resulting in a data breach involving customer payment card information in US District Court for the Northern District of California (Case No. 20-cv-00812).
- Design of employee monitoring and employee data-sharing programs in compliance with the GDPR and OSHA requirements. Act as the privacy counsel for workplace privacy issues concerning the processing of employee data.
- Develop and implement standardized information security and data governance policies to mitigate data processing legal risks under GDPR and CCPA.
- Oversee a national retailer’s cloud migration regarding privacy issues using AWS S3 bucket access right settings. Create corporate training for IT Teams based on Capital One Breach and involvement of non-malicious insider error.
- Advise on the collection, use, transfer, disclosure, and disposition of data in compliance with the law, policy, and best practices under US and foreign jurisdictions, particularly for controlling data ownership in complex Big Data projects.
- Work on privacy compliance on platforms used in decentralized marketplaces for trading of personal data collected through IoT devices and consumer questionnaires. Draft data usage clauses under CCPA’s service provider and customer structure.
- Negotiate SLAs regarding data ownership, availability, response time, resolution time, scorecards, and credits on IaaS, SaaS, and SIaaS applications.
- Provide counsel on data ownership and pro-customer vendor negotiations regarding data usage and aggregate data on the cloud through SLAs.
- Provide FTC Section 5 counseling on privacy issues (deceptive/unfair) for cognitive systems in customer care, case management, and marketing.
- Restructure cloud operations for cross-border data transfers based on global data sovereignty, data

localization, and government surveillance regimes. Coordinate the implementation of bring-your-own-key to manage data privacy on the cloud and prevent unnoticed government intervention.

- Advise a multinational energy company on global data sovereignty and data localization requirements; country-based risk and government surveillance practices in Asia-Pacific, Asia, and Europe.
- Provide counsel for GPS-data-based security product development for use in Europe, Canada, and the US; in respect of restrictions by GDPR, FTC, CCPA, and PIPEDA on the processing of GPS location, travel, and employee tracking data.
- Perform security risk assessment and risk management for an online financial institution (start-up) based on NIST SP 800-53 Rev.5 and PCI DSS.
- Supervise pen-testing on a smart-grid T-SCADA, and provide support on the implementation of Homeland Security Guidelines on Critical Infrastructure, legitimacy of the use of deception and counterattack strategies; and development of threat sharing channels to utilize federal law enforcement collaboration.
- Participate in Dentons Smart Cities Think Tank and support member-cities for contemporary developments, i.e., moral use of face recognition systems, use of AI, cybersecurity risks deriving from IoT AI, IoT-based SCADA in smart grids.

Activities and Affiliations

Memberships

- Atlantic Council
  - General Counsel
  - Member, Executive Committee
  - Member, Nominating & Governance Committee
- Middle East Institute
  - Board of Governors
- International Security Managers Association
- ASIS International
- American University Washington College of Law
  - Board of Advisors, Technology, Law & Security
- Association of International Petroleum Negotiators
- Texas A&M University
  - Chancellor's Advisory Board
  - George Bush School of Government and Public Service

Areas of focus

Practices

- Privacy and Cybersecurity
- Litigation and Dispute Resolution
- Arbitration
- Corporate
- Energy

Education

- George Bush School of Government and Public Service, 2012, Masters Certificate, International Affairs, Intelligence Emphasis
- Southwestern Law School, 1992, JD
- Texas A&M University, 1989, BA, History

Admissions and qualifications

- District of Columbia
- Solicitor, Senior Courts of England and Wales
- Texas
- US District Court for the Southern District of Texas