Summary of Skadden's Cybersecurity and Data Privacy Capabilities

Skadden

Content

Skadden's multidisciplinary **Cybersecurity and Data Privacy Practice** assists clients in navigating the rapidly evolving cybersecurity, privacy and technology landscapes.

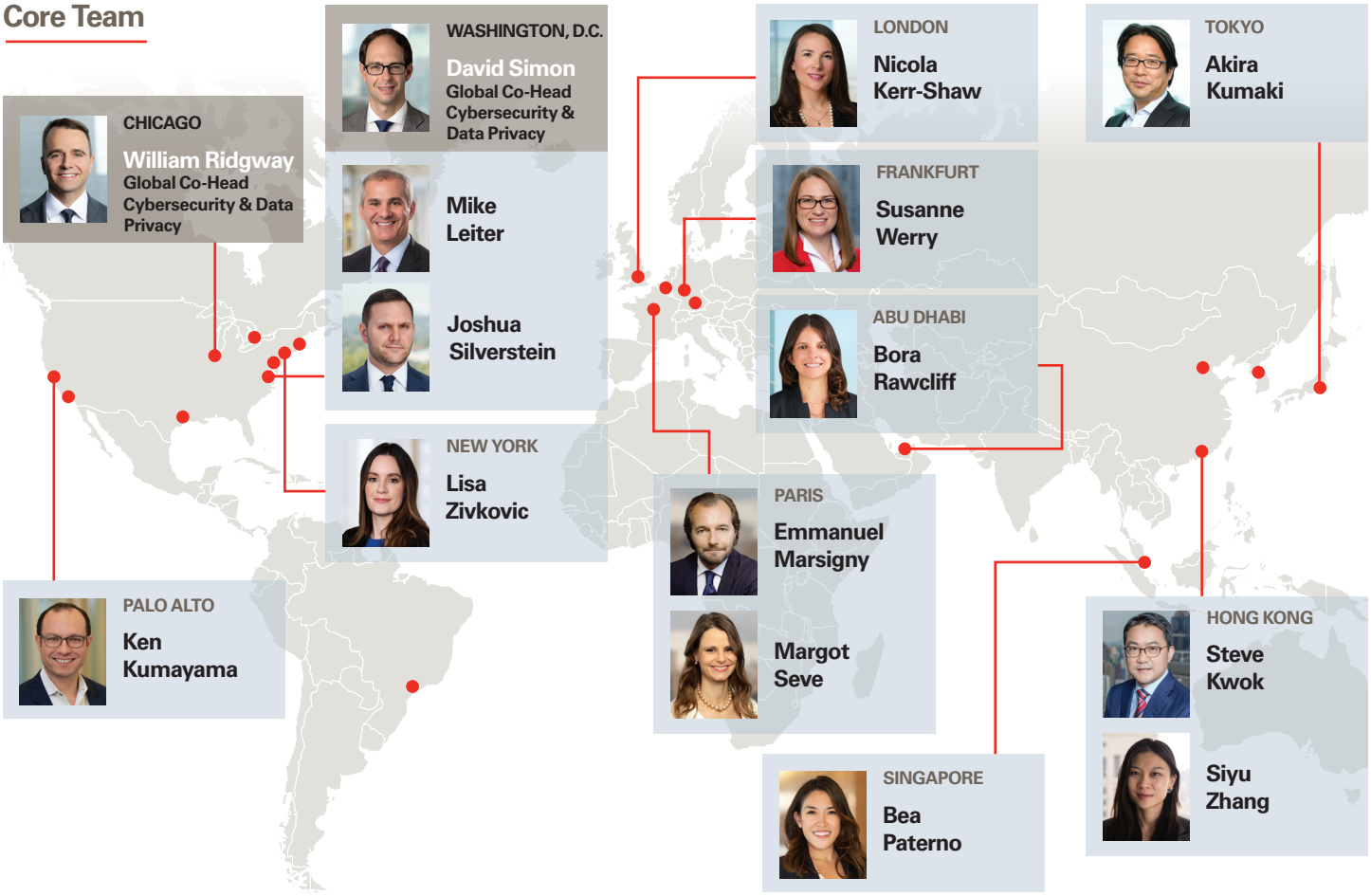
70+ professionals worldwide = **global one-stop shop** for:

- Cyber Incident Response and Preparedness
- Ransomware / Counter-Extortion
- Litigation and Enforcement Defense
- M&A Due Diligence
- Board and C-Level Guidance
- Regulatory Compliance
- Vendor and Supply Chain Diligence
- Artificial Intelligence

As seasoned "**breach coaches**," we provide practical, technical and operational guidance — during and after ransomware and other cyber events — based on **first-hand experience** managing the full spectrum of cyber and data privacy threats and incidents.

‘One-Stop Shop’
Global Platform, Global Reach

Core Team



CHICAGO

William Ridgway
Global Co-Head
Cybersecurity & Data Privacy

WASHINGTON, D.C.

David Simon
Global Co-Head
Cybersecurity & Data Privacy

Mike Leiter

Joshua Silverstein

NEW YORK

Lisa Zivkovic

PALO ALTO

Ken Kumayama

LONDON

Nicola Kerr-Shaw

FRANKFURT

Susanne Werry

ABU DHABI

Bora Rawcliff

PARIS

Emmanuel Marsigny

Margot Seve

SINGAPORE

Bea Paterno

TOKYO

Akira Kumaki

HONG KONG

Steve Kwok

Siyu Zhang

Cross-Practice Bench

SEC Reporting / Compliance

Brian Breheny

Raquel Fox

Antitrust / Competition

David Wales

Ingrid Vandenborre

Ken Schwartz

Bill Batchelor

Financial Regulatory

Mark Chorazak

Sebastian Barling

Insurance

Elena Coyle

Todd Freed

Peter Luneau

White Collar Defense / Investigations

Ryan Junck

Andrea Griswold

Anita Bandy

FDA Regulatory

Rachel Turow

Litigation / Arbitration

Meredith Slawe

Michael McTigue, Jr.

Archis Parasharami

Boris Bershteyn

Julie Bedard

Jennifer Permesly

Dan Jones

Kevin Ranlett

Zachary Faigen

Skadden Key Global Contacts

William Ridgway
Global Co-Head

1.312.407.0449
william.ridgway@skadden.com

David A. Simon
Global Co-Head

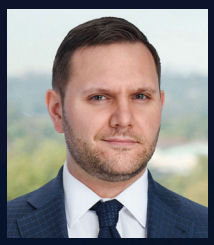
1.202.371.7120
david.simon@skadden.com

Steve Kwok
Hong Kong

852.3740.4788
steve.kwok@skadden.com

Nicola Kerr-Shaw
London

44.20.7519.7101
nicola.kerr-shaw@skadden.com



Joshua Silverstein
Washington, D.C.

1.202.371.7148
joshua.silverstein@skadden.com

Susanne Werry
Frankfurt

49.69.74220.133
susanne.werry@skadden.com

Cyber Incident Response

Skadden's Cybersecurity and Data Privacy Practice has handled some of the most significant cyber incidents on an international scale and counseled companies on major cyber breaches and incident preparedness across virtually every industry, including financial, health care, real estate, transportation, energy, chemical, defense and aerospace, telecommunications, tech and hospitality. With more than 70 lawyers globally, our Cybersecurity and Data Privacy Practice is a one-stop shop for companies' most pressing cybersecurity challenges. We advise victims of state-sponsored cyber activity, ransomware and other cyber extortion attacks, as well as breaches of health information, sensitive government information, intellectual property and personal data.

Market leaders. We are recognized as go-to counsel and breach coaches to *Fortune* 500 companies, stepping in to serve as cyber counsel and incident commanders when companies face ransomware or other disruptive cyberattacks. Drawing on our extensive experience across our worldwide platform, our global team manages the full spectrum of high-profile cyber and data privacy threats and incidents, often of a cross-border nature.

Dedicated service, 24/7/365. Our team is ready at a moment's notice to help companies navigate potentially catastrophic, increasingly sophisticated cyber threats. As seasoned "breach coaches," we handle time-sensitive, high-profile attacks by executing a battle-tested process to investigate the incident, limit its harm and command the response team's efforts to mitigate the company's legal, business and reputational risks. Our unified efforts are tailored to the client's size, cybersecurity maturity and existing processes; the incident's nature and scope; and the needs of customers, business partners, vendors, regulators and law enforcement officials across the globe.

Swift, coordinated action. Our ability to quarterback a crisis management plan is crucial when responding to a cybersecurity incident, which may require the help of forensic investigators, e-discovery professionals, threat actor negotiators, crisis communicators, asset recovery service providers, managed service providers and numerous other parties. Skadden's approach of quickly assembling and orchestrating collaborative teams of advisers is key to our successful track record on behalf of clients.

Practical insights. Skadden lawyers have served at the highest levels of the U.S. government, gaining experience that is extremely useful in managing and investigating complex cybersecurity incidents. This background is essential to our ability to craft and orchestrate a response plan that carefully considers government officials' incident notification expectations and enforcement and prosecutorial objectives.

Streamlined insurance process. Leveraging Skadden's strong relationships with the insurance industry, we work with providers throughout the incident lifecycle to facilitate the insurance process.

Skadden provides end-to-end support during the incident response with the help of a trusted network of experts, including by:

- **Preserving attorney-client privilege** and other protections through a tiered method that includes overseeing communication channels and retaining independent experts to maintain the confidentiality of sensitive information in the event of future litigation or enforcement proceedings.
- **Investigating the incident**, in collaboration with internal and external stakeholders, with an eye toward fully understanding the attack's scope and impact and ensuring that the investigation is conducted in a legally defensible manner.
- **Ensuring effective communication** with the media, vendors, customers, regulators and internal staff, by helping to manage communication lines and maintain clear, consistent messaging, to minimize the possibility of legal or reputational risk.
- **Identifying notice obligations** and coordinating notifications under relevant statutory, regulatory and contractual frameworks and managing the increasingly demanding, intricate and often conflicting notification processes across jurisdictions.
- **Documenting facts and actions**, carefully tracking everything from who learned of the incident and when, to the steps the company took to respond, under what can be highly unpredictable, high-stakes and complex circumstances.
- **Incorporating lessons learned** into cybersecurity preparedness policies and programs.

Cybersecurity and Data Privacy Capabilities

Cyber Incident Preparedness

Our attorneys work with boards, C-level executives and management teams to identify, assess and prepare for cyber risks before a ransomware attack or other breach occurs, by:

- **Developing custom incident response plans and cyber legal playbooks** to implement throughout the organization, including a robust governance framework.
- **Conducting gap assessments** to identify weaknesses and ensure the company's current practices are in line with cybersecurity best practices.
- **Developing and facilitating realistic cyber "war games" and tabletop exercises** to assess and enhance the organization's level of preparedness and resilience for an actual incident and inform potential updates to its incident response plan and playbook.
- **Collaborating closely with insurers**, drawing on our extensive experience with leading cyber insurance brokers and carriers, to support clients as they prepare for and respond to cyber incidents.

Board and C-Level Guidance

Regulators and private plaintiffs scrutinize a company's cybersecurity governance to assess whether chief information security officers had clear accountability and access to senior management and the board, and whether the board was sufficiently informed.

We help clients develop tailored cybersecurity governance practices and review governance that clients already have in place, advising on whether changes may be warranted to align with regulatory expectations and best practices.

Regulatory Compliance

- Cybersecurity, Privacy and AI Program Development
- Cybersecurity, Privacy and AI Gap Assessments
- Regulatory Watch Covering Key Developments and Implications

Our attorneys have deep experience advising clients on their obligations under regulatory regimes around the world, including with respect to cybersecurity, data protection, privacy and AI requirements, reporting and best practices.

We advise on compliance with a wide range of laws and regulations, such as:

- State privacy laws, including the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA).
- SEC cybersecurity rules.
- Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH).
- Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (ACTA).
- Children's Online Privacy Protection Act (COPPA).

Summary of Skadden's Cybersecurity and Data Privacy Capabilities

Continued

- CAN-SPAM Act, Telemarketing Sales Rule and Telephone Consumer Protection Act (TCPA).
- EU General Data Protection Regulation (GDPR) and UK GDPR.
- EU Network and Information Security (NIS) and NIS2.
- EU Digital Operational Resilience Act (DORA).

Our SEC reporting and compliance attorneys can quickly assess whether disclosure is required under SEC filings or as a result of the company's regulatory obligations, and draft any necessary disclosures.

Gap assessments. Skadden works closely with clients to help them understand the scope and applicability of regulations to their business and to design compliance programs that meet their legal obligations, including managing the evolving requirements of cross-border data flows.

Our attorneys conduct cybersecurity, privacy and AI gap assessments, reviewing existing governance through a litigation and enforcement lens and developing tailored compliance programs to align a client's governance with regulatory expectations and best practices.

Policies and procedures. As an increasing number of states and regulators now require formal written cybersecurity and privacy policies, we have experience creating and reviewing clients' policies, including:

- External-facing policies.
- Internal policies concerning cybersecurity and the use of personally identifiable information (PII).
- Statements to be used in marketing collateral regarding security policies.
- Written information security policies (WISPs).
- Data processing agreements (DPAs).
- Language regarding cybersecurity and data privacy to include in third-party contracts.

Regulatory watch. Skadden tracks key cyber, privacy and AI developments at the state, national and global levels to inform our clients about important regulatory changes and to look over the horizon.

Litigation and Enforcement Defense

Skadden offers a sophisticated practice — led by former federal prosecutors and experienced trial and appellate lawyers — focused on cybersecurity and privacy litigation and government and internal investigations.

We have vast experience in the types of litigation that arise in the aftermath of an attack, such as:

- Class actions (filed even in the absence of facts or actual proof of damages).
- Contractual disputes.
- Shareholder derivative actions.

We are uniquely equipped to counsel clients in consumer class actions following a breach.

Skadden defends clients facing significant matters brought by enforcement agencies and conducts internal investigations for boards of directors, audit and special committees and management, often in their most sensitive situations.

Our team includes former government officials who have extensive experience with:

- FBI Cyber Division.
- Computer Crime and Intellectual Property Section of the Department of Justice.
- Secret Service.
- Department of Defense.
- Department of the Treasury.
- Department of Homeland Security.
- Various independent regulatory agencies.

Skadden is ranked as a leading firm in the Privacy & Data Security: Litigation category in *Chambers USA*.

Summary of Skadden's Cybersecurity and Data Privacy Capabilities

Continued

M&A Due Diligence

Due diligence has long been a critical tool for uncovering and protecting against key risks in a transaction. Cybersecurity due diligence requires a custom approach.

As with any diligence effort, the scope will depend on the transaction timeline as well as the target company's industry, the value of its digital assets, its regulatory environment and its cyber-risk profile.

Our team has developed due diligence questions that help clients assess these risks.

Vendor and Supply Chain Diligence

We examine clients' vendor management processes to ensure that appropriate steps are in place to assess cybersecurity risk.

Our attorneys draft, negotiate and review our client's third-party vendor agreements — including cross-border data processing, sharing and transfer provisions and global supply chain contracts — to determine if the client is adequately protected with respect to cybersecurity incidents.

We also help clients assess their data breach notification obligations after an incident occurs. Our experience includes handling outsourcing transactions and ongoing contract governance.

Artificial Intelligence: Security and Privacy Issues

Skadden helps companies successfully traverse the burgeoning security, privacy and compliance challenges posed by the development and use of cutting-edge AI technologies and automation.

- **Data security and privacy.** Our attorneys are well equipped to advise clients on AI-related cybersecurity vulnerability management, assessments and disclosure programs.
- **Governance and compliance.** Skadden has extensive experience in reviewing, developing and implementing effective ethics and compliance programs and sound corporate governance practices, including advising and training management teams and boards on AI-related policies, procedures and accountability frameworks.
- **Regulatory tracking.** We carefully track evolving regulatory and other standards related to the global AI landscape.

The Americas
Boston
Chicago
Houston
Los Angeles
New York
Palo Alto
São Paulo
Toronto
Washington, D.C.
Wilmington

Europe
Brussels
Frankfurt
London
Munich
Paris

Middle East
Abu Dhabi

Asia Pacific
Beijing
Hong Kong
Seoul
Singapore
Tokyo