Hogan Lovells

Cyber Risk Services

Hogan Lovells' Technical and Risk Management Consulting Services

The cyber threat landscape is evolving daily. To stay in front of it, you need comprehensive, timely advice and solutions to your organization's unique challenges. That's why our Cybersecurity Solutions team is expanding its dedicated group of technical and risk professionals who work side-by-side with our market-leading lawyers. Clients receive tightly integrated and complementary legal, technical, and management counsel, creating a seamless experience appropriately protected by attorney-client privilege.

The technical knowledge and training of our consultants and lawyers allows us to work directly with a client's IT security team, as well as in-house counsel, with no lost time for "translation" of specialized terminology or concepts. And our experience within, and working with, law enforcement and other government agencies enables us to counsel and support internal investigations, litigation, and other external interactions with practical, informed advice.

Our technical professionals, consultants, and lawyers work with you end-to-end on planning, preparation, and response issues. In particular, our consultants partner closely with our lawyers on:

- **Program development.** We evaluate cyber threats; analyze preparedness; review policies, procedures, and technical capabilities against best practices; develop policies and procedures for oversight and management of risk; and evaluate vendor cybersecurity practices.
- **Incident and crisis response.** We develop plans and procedures for investigating and responding to cybersecurity incidents, testing response capabilities, managing the response, providing technical and procedural recommendations, and supporting incident response, investigations, and litigation.
- **Compliance (e.g. HIPAA, ITAR, NNPI).** We develop policies, procedures, and technical cybersecurity requirements needed to comply with regulations and major industry standards; review existing policies, procedures, and capabilities; and recommend mitigations necessary to comply with regulations.
- **Training and Awareness.** We evaluate threats from employees and contractors; analyze the capability to protect against inside threats; evaluate internal cultural awareness; and recommend, develop, and deliver cybersecurity awareness and best practices training.

Taking on your cyber challenges

You'll want to know that the consultants and lawyers you work with have the technical and legal experience to see you through every phase. For years we've worked with companies, big and small. A few examples of how we've helped include:

Client: Major U.S. Retailer

Need: Technical oversight of third-party forensics report preparation

How we helped: After a major payment card breach, our technical consultants reviewed and advised on the scope and conduct of a third-party technical investigation, conducted a technical review of multiple drafts of the forensics report, worked with forensics experts, and helped shape the report's favorable findings and practical recommendations.

Client: Major U.S. Company

Need: Summarize complex technical facts in support of legal defense

How we helped: The company suffered a data breach involving more than tens of millions of records containing sensitive personal information. Our management and consulting team and lawyers created a summary of the key legal arguments and a plain-language description of the technical and business facts that supported them, which was then used by the client to prepare its defense and settlement strategy.

Client: Major Health Insurer

Need: Confirm the absence of cyber attackers in their systems

How we helped: Our lawyers helped the company retain a respected forensics firm to conduct a technical scan of the client's systems. Our cybersecurity consultants participated in the scoping and review meetings and reviewed the resulting report, providing the client with the reassurance that the work performed would help demonstrate, as much as reasonably possible, that all steps had been taken to protect the client's data and systems.

Client: Major Cable and Internet Services Provider

Need: Assessment of the client's cybersecurity risk management approach

How we helped: After interviewing the chief information security officer, chief information officer, chief operating officer, and other key stakeholders, we recommended the client adopt a governance framework and approach more aligned with industry standards and legal frameworks.

Client: Major U.S. Defense and Government Services Contractor

Need: Comprehensive assessment of existing cybersecurity program and detailed recommendations for improvement

How we helped: Our client is responsible for protecting a wide variety of sensitive government and private sector data. We assessed its existing policies and practices against both the NIST Cybersecurity Framework and a range of additional industry "best practices." Our lawyers and cybersecurity consultants designed a comprehensive legal and technical assessment, interviewed senior executives and technologists, and reviewed all organizational cybersecurity-related policies and procedures. We then produced a report for our client detailing the legal, policy, and technical steps they could take to further advance their commitment to being an industry leader in cybersecurity.

For more information, contact:

Jeff Lolley, Managing Principal, Cyber Risk Services
+1 202 637 5567 jeffrey.lolley@hoganlovells.com

Deen Kaplan, Partner
+1 202 637 5799 deen.kaplan@hoganlovells.com

Harriet Pearson, Partner
+1 202 637 5477 harriet.pearson@hoganlovells.com

www.hoganlovells.com