WILSON ELSER

Cybersecurity Crisis Management & Emergency Response

Businesses continually strive to strike a balance between furthering their objectives and managing the accompanying risks. Yet, even with the soundest strategies, this delicate equilibrium can be jarred by a sudden catastrophe that threatens business momentum, customer confidence and even a company's financial foundation.

Combining proactive defense capabilities with years of proven litigation experience, Wilson Elser handles crisis management and emergency response for countless clients. Specifically with respect to **transportation accidents**, **product contamination and recalls**, **cyber-attacks** and other **catastrophic events**, we offer the highest-caliber representation in the industry and among insurance markets.

For several of our practice areas and in many key venues nationwide, we assemble "go teams," comprising combinations of attorneys, accident reconstructionists, independent adjusters, investigators, forensic experts, diagnostic engineers, criminal defense attorneys, public relations experts and other specialists. They typically are on site and fully engaged within hours – or even minutes – of an event. As best serves our clients' needs, we also draw on the vast resources of the broader firm, including 41 offices in the United States, another in London and dozens of key international locations afforded by our founding membership in Legalign Global.™

24/7 /365
National Coverage

While technology has enabled an interconnected global economy, it also has given rise to profound risks for consumers and companies alike. An increasing number of actors from virtually every part of the globe have exploited cybersecurity vulnerabilities, disrupting businesses, corrupting data, co-opting personal information, and otherwise wreaking havoc on organizations and national economies. In the evolving cyber landscape, instances of neglect have led to equally devastating results. These often involve uninformed or careless leadership, employees or third-party vendors.

An inconvenient afterthought as recently as a decade ago, the explosive growth of e-commence and increased dependence on digitized data has catapulted cybersecurity to the forefront of business plans, legislative acts and federal regulations as companies and government entities deepen their presence and investment in the complex and evolving digital landscape.

CYBER BREACH

Decisions made immediately following a data breach can significantly impact outcomes. For well over a decade, Wilson Elser's core team of talented partners, assisted by associates and paralegals, has handled breach response and other sensitive situations arising from the misuse of computers and related technology. We understand that data intrusions – real and perceived – require decisive and appropriate action. Following reports of a breach, our Cybersecurity & Data Privacy practice team members begin a triage process designed to immediately reduce exposure. Every breach has a distinctive set of characteristics and surrounding circumstances. Our experience allows us to respond swiftly and categorically to each. We regularly oversee forensic analyses, engaging experts specially chosen to enhance protection of privileged and confidential communications, determine the cause of the breach and identify what data was at risk. Results guide the implementation of measures designed to comply with legal obligations and prevent additional data intrusions.

Depending on the situation, we can pursue other protective steps, such as:

- Communicating with operational, legal and executive leaders regarding the breach
- Advising when and how to involve law enforcement and, where appropriate, engage law enforcement in a responsible way
- Crafting notification letters based on the varying requirements of states and countries
- Providing options and recommendations on the structure and kinds of assistance provided to individuals whose sensitive information may have been exposed
- Deploying tested public relations strategies in communicating with stakeholders and the press.

CYBER DEFENSE & LITIGATION

With arguably more senior litigating partner experience than any other law firm in the United States, our litigators handle the most challenging and technical cyber cases. We sort through the complex technical and legal issues that characterize this practice, often serving as defense or coverage counsel on matters such as:

- Cybersecurity preparedness
- Data breach
- Business-to-business litigation
- Violations of privacy rights
- Technology errors and omissions
- Web-based media issues
- Breach of contract
- Class actions
- Fraud
- False advertising
- Defamation
- Advertising and media exposure
- Negligence
- Unfair trade practices/ consumer protection violations.

We seek cost-effective results for our clients through early assessment and negotiations, alternative dispute resolution methods or summary judgment motions. When early resolutions are not possible, we have the skill and experience to resolve cases in court. In fact, we count among our ranks some of the finest trial attorneys in the country.

RISK MANAGEMENT

Many U.S. organizations are subject to compliance with various state, federal and, increasingly, international cybersecurity and privacy laws, in addition to the EU General Data Protection Regulation (GDPR) with its extraterritorial reach to U.S. businesses. We assist clients with drafting and updating their privacy policies and procedures to comply with applicable laws and regulations and work with them on crafting a detailed incident response to help ensure adequate preparation before a cyber-attack occurs.

Our risk management services additionally include training clients and their employees on cyber threats and evolving privacy laws and make extensive use of interactive data breach simulations.

Our attorneys assist clients in responding to inquiries by state and federal authorities with whom we have frequent interaction and, in some cases, longstanding ties. Among our ranks are former government attorneys for the U.S. Department of Justice and state attorney's offices who contribute valuable, first-hand perspectives on related authorities. As it best advances our clients' objectives, we will interact with one or more of the following:

- The Federal Bureau of Investigation's Cyber Division, including local agents to coordinate notification protocols for clients who are victims of cybersecurity incidents
- The Internal Revenue Service, including local agents with direct contact to the IRS Task Force on Cybercrime, allowing for quicker notification of tax-related identity theft and for flagging potential victim files to prevent the filing of false tax returns
- The U.S. Secret Service and Department of Homeland Security through the coordination of investigations and sharing of information
- The U.S. Department of Health and Human Services, Office of Civil Rights, including the Office of HIPAA Compliance, allowing for early interpretation of new regulatory guidance, along with local contacts in all regional offices.

Case Studies

- **We served as breach counsel in connection with a cybersecurity incident involving nearly two million registered voters**. An unauthorized intruder gained potential access to personal information of voters, some of which was reportedly available on the "Dark Web." We worked closely with the client, municipality and state attorney general to ensure prompt notification and remediation to affected individuals, including media notice. Despite the high-profile nature of this incident and the news reports surrounding it, our client successfully escaped any litigation or claims by affected individuals, third parties or regulators.

- **We represented a nationwide restaurant chain in connection with a data breach involving more than 250,000 customer credit card numbers across more than 250 restaurant locations**. The breach stemmed from a third-party credit card payment processor that failed to comply with Payment Card Industry Data Security Standards (PCI-DSS). We worked closely with state regulators and prevented our client from being subjected to a formal investigation or enforcement action by the state attorney general in connection with the data breach.

- **In a case of first impression in the Fifth Circuit, we obtained dismissal of a cybersecurity putative class action involving a hospital system data breach**. The lawsuit alleged that the breach affected 405,000 patients and employees who were seeking damages in excess of $225 million. We argued the putative class had no Article III standing to sue because they failed to demonstrate a heightened risk of future identity theft or fraud. The district court dismissed the lawsuit while providing plaintiffs the opportunity to re-file their suit in state court. We again successfully obtained a dismissal of the lawsuit.

- **We represented a back-up storage equipment and software provider in a suit alleging that our client's installation of software corrupted a third party's computer systems, resulting in the loss of data for the clients of an internet service provider**. After prevailing on a particular motion to dismiss and enforcing the limitation of liability provision in our client's contract, we resolved the $36 million damages claim against our client for pennies on the dollar.

- **We represented a U.S. company (client) that was the victim of a business email compromise resulting in multiple fraudulent wire transfers totaling hundreds of thousands of dollars to a bank account in Hong Kong**. The client hired a third party to provide accounting services (vendor). The vendor's email account was hacked by an unknown third party (intruder). The intruder sent a series of spoofed emails that appeared to come from the client, instructing the vendor to wire funds in excess of $700,000 to Peru, Japan and Hong Kong. We oversaw a forensics investigation of the client to confirm that its email system had not been compromised. We asserted claims on behalf of the client against vendor for gross negligence in failing to follow established protocol by wiring large sums to foreign banks without verification. We successfully recovered $250,000 from the vendor after drafting a complaint and threatening to file suit. In addition, we partnered with local counsel in Hong Kong to commence a legal proceeding against the accountholder to recover the missing funds still remaining in the Hong Kong bank account. Wilson Elser obtained a final judgment in the Hong Kong proceeding and garnishment order requiring the Hong Kong bank to turn over proceeds totaling $200,000. Our team worked with the Hong Kong police to enforce the garnishment order. In short, we successfully recovered $450,000 of the client's missing funds. The balance was covered by the client's cyber liability insurance policy.

- **We represented a health insurance third party administrator in Ontario, Canada that was the victim of a business email compromise (BEC) resulting in a fraudulent wire and suspected compromise of personal information (PI) of thousands of individuals residing in various foreign jurisdictions (including Canada, India, EU, Cayman Islands and Bahamas).** The client detected a BEC when hundreds of phishing emails were sent from the email account of its Human Resources Director. We oversaw a forensics investigation, which revealed that the email accounts of six (6) other client employees also had been accessed by an unknown intruder with a foreign IP address from Turkey. The forensics investigation also revealed that the intruder synched (downloaded) the contents of these email accounts, which contained extensive PI of thousands of individuals. We assisted the client in reporting the incident to foreign privacy regulators, including the U.K. Data Protection Regulator (Information Commissioner's Office or ICO) in compliance with GDPR notification obligations. The ICO closed its investigation without taking action. Wilson Elser also partnered with local counsel in Canada to document a risk assessment as required by Canadian privacy law (PIPEDA) and to confer with the Canadian privacy commissioner. Finally, Wilson Elser assisted the client in reporting the incident to residents of India. This matter concluded without any regulatory action or complaints by individuals.