OUR PRACTICE

Data Incident Response

Your First Call in a Cyber Crisis: When a cyber incident strikes, time is everything. Baker Donelson's seasoned Incident Response Team is ready 24/7/365 to guide clients through every phase of a data breach – from managing and coordinating forensic investigations, crisis communications, regulatory reporting, complying with individual notification requirements, and litigation defense. We provide real-time legal, technical, and business-focused advice designed to minimize disruption, protect what matters most, and keep your business moving forward. With deep experience handling all types of incidents, including ransomware attacks, business email compromises, insider threats, and supply chain breaches, we offer clear, calm, and strategic guidance that is tailored to your organization's needs when you need it most.

Our Incident Response Team acts quickly and decisively, leveraging our trusted network of forensic investigators, breach notification vendors, call centers, crisis communications firms, and cyber insurance partners to help clients respond with confidence – whether the issue affects 500 or 5 million individuals.

We represent clients across all industries, including some of the most highly regulated sectors, such as financial services, health care, insurance, education, and energy. Whether advising a Fortune 100 company on a nationwide ransomware attack, assisting a regional health care provider with HIPAA breach reporting, or guiding a startup through its first incident, we tailor our response to meet the unique demands of each situation. No matter the size or complexity of the matter, our team brings the same level of focus, responsiveness, and strategic insight to every engagement.

Recognized as an authorized NetDiligence® Breach Coach, our team is a go-to advisor for organizations across industries, including health care, financial services, retail, education, and critical infrastructure. We don't just know the law – we know how breaches really unfold and how to protect your brand, your customers, and your bottom line.

Comprehensive Cyber Incident Response Services

At Baker Donelson, our Incident Response Team delivers comprehensive support at every stage of a cyber incident or data breach – from first alert to full recovery – including:

- communicating on behalf of our clients with state and federal law enforcement agencies with whom we have established relationships;
- appropriately working with industry experts to assist with detection, containment, and recovery;
- managing communications with vendors, employees, customers, and other key stakeholders;
- collaborating with established expert third-party resources to advise clients on ransomware negotiations;
- responding to any state and federal government investigations or enforcement actions that result from an incident;
- coordinating e-Discovery efforts when exfiltration is identified;
- providing analysis to assist in developing post-incident remediation; and
- representing clients in ensuing litigation, including class action cases, involving data incidents.

Success Stories

Our experience spans hundreds of cyber incidents, from complex, multijurisdictional breaches to targeted attacks on small and mid-sized organizations. We are trusted by clients across the country from all industries to lead them through their most sensitive and high-stakes cybersecurity events. The following are just a few examples that highlight how our team has delivered strategic, results-driven guidance to help clients contain threats, manage regulatory exposure, and protect their reputations when it mattered most.

Swiftly Navigated a Complex Ransomware Crisis

Successfully led an incident response team for a medical information technology company after a ransomware attack, mitigating operational disruptions and ensuring compliance with HIPAA. Oversaw regulatory interactions, breach notifications in multiple states, coordination with law enforcement, and effective crisis communications – minimizing litigation risks and restoring stakeholder confidence.

Comprehensive Management of Multistate Ransomware Incident

Directed the response to a ransomware attack on a national transportation and logistics company, ensuring compliance with breach notification laws across 30 states. Managed law enforcement interaction and oversaw crisis communications, providing strategic leadership during a critical business interruption.

Resolved a High-Stakes Wire Fraud Incident

Successfully represented a U.S. distribution company for an international lubricant brand following a phishing attack resulting in substantial wire fraud. Navigated complex privacy law requirements, including GDPR and U.S. regulations, while coordinating breach notifications in more than 14 states and coordinating with law enforcement to address the cybercrime.

Mitigated a Large-Scale Data Incident for a National Bank

Represented a national bank during a vendor data breach affecting hundreds of corporate clients and more than 250,000 individuals. Guided the bank through sensitive customer communications and regulatory obligations, preserving trust and minimizing reputational harm.

Secured Schools After a Ransomware Attack

Successfully negotiated and resolved a ransomware attack on a school board that disrupted the education of more than 5,000 students. Managed crisis communications and guided the organization through restoring operations with minimal long-term impact.

Defended an E-Commerce Leader in Regulatory Investigations

Supported a leading e-commerce company after a phishing attack compromised multiple employee email accounts. Provided guidance on regulatory compliance under PCI-DSS and successfully responded to state attorneys general investigations, ensuring continuity in operations.

Protected a Hospital System in a Federal Investigation

Achieved a favorable resolution for a large hospital system following a data breach, navigating an Office for Civil Rights (OCR) investigation, and ensuring compliance with HIPAA regulations while avoiding adverse actions.

Addressed Employee Data Theft for a Brokerage Firm

Advised a national brokerage firm on regulatory and individual notification obligations following the theft of electronic data by an employee, ensuring regulatory compliance and minimizing potential legal repercussions.

Assisted With the Recoupment of Stolen Funds for a Banking Client

Represented a bank in a wire fraud incident, successfully negotiating the return of a significant portion of stolen funds.

Resolved Patient Data Theft for a Mental Health Facility

Assisted a mental health facility in responding to a former employee's theft and misuse of patient records, ensuring proper notification and remediation efforts to protect sensitive patient information.

Remediated a Data Breach for Automotive Dealerships

Advised a network of automotive dealerships on breach notification and remediation after a theft of employee data. Implemented measures to ensure regulatory compliance and reduce future risks.

Resolved Data Breach Litigation

Successfully defended a national company in a class action lawsuit resulting from a phishing attack. Secured a favorable resolution that minimized financial and reputational damage.

Obtained Exoneration in a Large-Scale OCR Investigation

Represented a business associate during an OCR investigation of a data breach potentially impacting 3.5 million individuals. Successfully documented the client's robust security protocols, resulting in the OCR dismissing the investigation.

Represented a National Health Care Supplier in a Ransomware Attack

Represented the client in response to a ransomware attack that resulted in notification to more than 2 million individuals. Successfully responded to both state and federal (OCR) investigations of the incident; all investigations were closed with no adverse action against the client.

Managed the Response to an Incident for a Government Contractor

Oversaw an incident for a government contractor, including engaging and working with crisis communication experts to draft and manage employee, media, and stakeholder communications. Assessed notification obligations to, and managed communications with, multiple government agencies given the client's government contracts and funding. Successfully resolved the matter without any individual notifications being required.

Team Member Credentials

Our team holds certifications from the International Association of Privacy Professionals (IAPP) – the world's leading organization for privacy professionals – as well as other respected industry credentialing bodies. These certifications reflect our deep understanding of global privacy laws, data protection frameworks, and incident response best practices. In high-pressure breach scenarios, our clients benefit from working with professionals

who not only know the law but also have the technical fluency and regulatory insight to respond swiftly and strategically. Our team's credentials include:

- Artificial Intelligence Governance Professional (AIGP)
- United States-Focused Certified Information Privacy Professional (CIPP/US)
- Europe-Focused Certified Information Privacy Professional (CIPP/E)
- Canada-Focused Certified Information Privacy Professional (CIPP/C)
- Certified Information Privacy Technologist (CIPT)
- Privacy Management-Focused Certified Information Privacy Manager (CIPM)
- GIAC Law of Data Security & Investigations (GLEG)
- Privacy Law Specialist (PLS)
- Payment Card Industry Professional (PCIP) Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Qualified Technology Expert (QTE)

Baker Donelson Cyber Readiness Resources

We believe that preparation is the best defense. To support our clients and the broader business community, we provide practical, easy-to-use resources designed to strengthen cyber-readiness and streamline data breach response efforts. Our materials reflect real-world experience and industry best practices. Whether you are building a program or navigating an incident, these free tools are here to help you stay ahead.

- Checklist for Preparing an Incident Response Plan
- Tabletop Exercise Best Practices
- The Role of Third Parties in Cyber Incidents
- Cyber Best Practices
- Third-Party Vendor Cybersecurity Due Diligence Checklist
- Basics of Ransomware
- Five Components of SEC Cybersecurity Disclosure Rules