

OUR PRACTICE

Information Security

Baker Donelson has been recognized as an authorized NetDiligence Breach Coach® signifying it as a top tier law firm for Data Security, Privacy and Incident Response. Sophisticated cyber attacks are quickly becoming one of the most prevalent issues affecting modern businesses. With the rise of critical data breaches across the world, Baker Donelson is aware of our manufacturing clients' need to be prepared in advance for cyber attacks. We understand how sensitive and critical a manufacturer's data is, whether it relates to human resources, technological and business information or e-commerce. We provide our clients with information privacy and security management plans that recognize their specific business needs while seamlessly incorporating law, business and information technology requirements into one package. We coordinate communication between stakeholders to identify and proactively manage risk effectively; help reduce governance and compliance expenditures through integration of legal requirements into business processes; and apply information security and privacy technology standards effectively and cost-efficiently.

In addition to assisting our clients in proactively responding to cyber security threats, our team is also available to assist clients who are targets of a data breach by providing security incident and crisis management support. We make ourselves available to our clients through all stages of a data breach, from the initial alerting of the event to post-response and future prevention.

Our multi-faceted approach to information security management helps organizations maximize their return on technology and related investment through cost savings, enhanced profits and innovation. Our services include:

- Security incident response plans
- Information privacy and security compliance plans
- Business continuity and disaster recovery plans
- Data governance/compliance plans – Advise boards of directors and management on technology and other issues engendered by the Sarbanes-Oxley Act, the Foreign Corrupt Practices Act and other international, federal and state laws and regulations, as well as marketplace requirements
- Document retention and destruction programs (including processes consistent with the new eDiscovery rules)
- Government contracts and critical infrastructure – Advise on agency and governmental entity requirements, as well as on RFP, RFQ and RFI responses
- Outsourcing – Advise on legal, regulatory and marketplace requirements for suppliers, vendors and the companies that hire them
- Policies, procedures, standards, baselines and guidelines
- Risk management
- Transactions – Due diligence, gap analyses, integration and interoperability issues; negotiation of appropriate representations and warranties; and transferability of information under international, federal and state laws and regulations
- Contract preparation and review – Determine compliance with international, federal and state laws and regulations, as well as marketplace requirements

Learn more about our Data Protection, Privacy, and Cybersecurity Practice [here](#).

