CYBERSECURITY AND DATA PRIVACY

Protect. Prepare. Respond. Defend.

Protecting your network means safeguarding the very core of your business. Every system can be vulnerable to attack. Having a seasoned team that keenly understands the legal, regulatory and technical triad of cybersecurity and data privacy is critical to mitigating risk and securing your business. Having the most up-to-date privacy policies, procedures and compliance program has never been more important.

What We Do

Our experience in cybersecurity and data privacy is unrivaled, having assisted numerous organizations in both the public and private sectors in planning for, responding to, and recovering from incidents. This vast experience equips us with the unique ability to quickly identify the root cause of an issue, provide immediate technical and legal advice and forecast risks and liabilities that organizations might face in the future. Our security professionals conduct in-depth data analysis to identify potential vulnerabilities and threats, helping to inform legal strategy and decision-making.

The ability to make informed decisions in the face of crises is critical, and our insights provide just that. Our collaboration extends to a diverse range of professionals, including forensic teams, ransom negotiators, payment agencies, crisis communication experts, mailing and call center vendors, brokers, and insurance providers. This collaborative approach streamlines our incident response process. Ensuring an effective response goes beyond mere legal compliance; it's about bringing the right experience and partners to bear to get you back to business. We take charge, leading efforts to constantly refine strategic plans that aim to identify, contain, assess, mitigate, and remedy any issue.

In addition to our response services, we also specialize in preparing businesses for potential data incidents or breaches, tailoring our approach to best fit your business model. Our comprehensive approach to cyber protection and preparedness includes several layers. At the core of our strategy are robust privacy, security, and breach notification protocols. We also emphasize the importance of a well thought-out incident response and emergency preparedness plan. Due diligence in vendor, supplier, and customer relationships, a thorough cyber insurance assessment, all-encompassing IT safeguards, and fostering employee awareness through regular training are also integral parts of our approach.

IS YOUR COMPANY FACING CYBERSECURITY OR DATA PRIVACY CONCERNS?

Our dedicated team of attorneys and policy advisors stand ready to provide legal guidance rooted in technological expertise. Contact us today at cyber@bipc.com.

How We Can Help You

Incident Response Readiness and Compliance

We assist companies in developing and refining incident response plans offering hands-on exercises with realistic data breach scenarios tailored to individual clients and collaborating with forensic and crisis communication experts to train response teams effectively. Our Cyber Response Team offers 24/7 support. Beyond legal advice, our team will also help to ensure that your IT systems and processes are compliant with various cybersecurity regulations. This includes conducting technical audits and providing recommendations for improvement.

Digital Risk Advisory

We guide organizations of all sizes through inquiries and assessments by regulators, state attorneys general, federal agencies, and international data protection authorities. Additionally, when a security incident results in a lawsuit, we work closely with our clients and our cyber litigation team to ensure that the initial incident response insights feed into a robust defense strategy.

Cybersecurity Advisory

Our mission is to make our clients breach-ready and resilient. Drawing from vast experience and analyzing hundreds of cyber threats, we aid organizations in enhancing their operational framework. This involves:

- Advising and assisting in crafting industry-specific regulatory compliance programs.
- Crafting risk-based security strategies, often using insights from third-party security firms and our internal technical expertise to provide comprehensive recommendations.
- Undertaking “reasonable security” evaluations to defend against potential legal and regulatory challenges.
- Addressing threats such as ransomware, business email compromise, social engineering, third-party and supply chain vulnerabilities, online account breaches and unauthorized access, bolstered by in-depth data analysis from our technical team.
- Assisting in due diligence for corporate transactions, including pre-acquisition assessments and post-acquisition integration planning.
- Streamlining vendor management and technology contracts and brokering major agreements involving advanced security technologies.
- Establishing comprehensive cybersecurity risk management programs and collaborating with corporate leadership at all levels. This includes setting up foundational security measures, charting cybersecurity roadmaps, and gauging cybersecurity maturity.
- Assisting publicly traded companies navigate the new SEC cyber rules.

Privacy and Data Security Litigation

In today’s digital world, the protection of data and personal information is of paramount importance. Cybersecurity breaches and data privacy violations can have severe consequences for individuals and organizations alike. If a breach does take you to the courthouse or finds you defending actions by regulatory agencies, our litigation team – highly experienced in post-breach suits – will defend you in any form of litigation in any venue, whether in single-plaintiff lawsuits, class actions, or actions brought by regulatory authorities. We treat privacy and data security litigation as a distinct legal field, recognizing the specialized knowledge necessary for achieving success in such cases. Our team of litigators possesses an in-depth understanding of the key laws that play a pivotal role in privacy and data security litigation. These include the federal Electronic Communications Privacy Act, encompassing the Wiretap Act and the Stored Communications Act, as well as the Video Privacy Protection Act, Fair Credit Reporting Act, and Telephone Consumer Protection Act. We are also well-versed in the state-level counterparts to these statutes, state consumer protection laws, and the common law privacy torts.

Working with Clients Across Multiple Sectors

Healthcare | Life Sciences | Education Institutions | Financial Institutions | Security Alarm Companies
Insurance Companies | Manufacturers | Hospitality Industry | Government Entities
Boards of Elections | Energy and Public Utility Companies | Children and Youth Services | Retailers
Liquidation Services | Emergency Medical Services | Critical Infrastructure

Advancing Our Clients' Goals

As a NetDiligence Authorized BreachCoach®, Buchanan is nationally recognized as a top-tier firm in the area of cybersecurity incident response. We have assisted publicly traded companies, private companies, government agencies, and organizations of all sizes that are facing cybersecurity incidents—including ransomware and extortion, "downstream" supply chain breaches, wire fraud, business email compromise, system vulnerabilities, and malicious insiders.

Defense Following a Cybersecurity Incident

We helped financial institutions, publicly traded companies, critical infrastructure, universities, and healthcare providers respond to the full spectrum of cybersecurity incidents.

B2B and B2C Companies of All Sizes are at Risk

Threat actors target businesses of all sizes, looking for ways to lock up their critical IT systems and data and demand ransom payments for release. When critical vendors are attacked, companies may lose essential services or be forced to suspend services to their customers. We assist clients in seeking redress from their third-party service providers who failed to maintain adequate security safeguards.

Working with Government Entities

The Buchanan team represented a public sector victim of the Accellion breach involving large data files with both structured and unstructured data, requiring extensive forensic search for personal information and multiple forms of notification to over 1.5 million individuals. We also assisted a state department of occupational licensing to navigate a vulnerability in third-party software involving notification to approximately 600,000 individuals.

Publicly Traded Companies Face Unique Risks

We assisted a Fortune 500 company respond to and recover from a complex ransomware attack by a highly sophisticated threat actor. We managed the work of 6 third-party vendors, advised on cybersecurity policies and best practices across three subsidiaries, and coordinated with federal law enforcement to bring the matter to a swift conclusion. We assisted in materiality determinations, advised on director and officer trading concerns, managed multiple SEC inquiries, and leveraged our expertise to minimize the risk of class action and derivative litigation.

Healthcare Institutions and Social Welfare Organizations are Always High Risk

We helped a hospital improve protocols for protecting customer and proprietary information, including developing enhanced employment and confidentiality agreements and privacy policies. We obtained dismissal of an investigation by the Department of Health & Human Services Office of Civil Rights with no further action when the Emergency Medical Services unit of a county sustained a breach of protected health information. We represented multiple children and youth services organizations when their protected client health records were exposed on the internet – reviewing the potentially compromised records to determine scope, preparing notification letters to affected individuals, and addressing questions on vendor responsibility and contractual obligations.

SUE C. FRIEDBERG
Co-Leader of Buchanan's Cybersecurity and Data Privacy Group
sue.friedberg@bipc.com
412 562 8436

MICHAEL G. MCLAUGHLIN
Co-Leader of Buchanan's Cybersecurity and Data Privacy Group
michael.mclaughlin@bipc.com
202 452 5463

KURT M. SANGER
Cybersecurity Counsel
kurt.sanger@bipc.com
212 440 4487