Buchanan

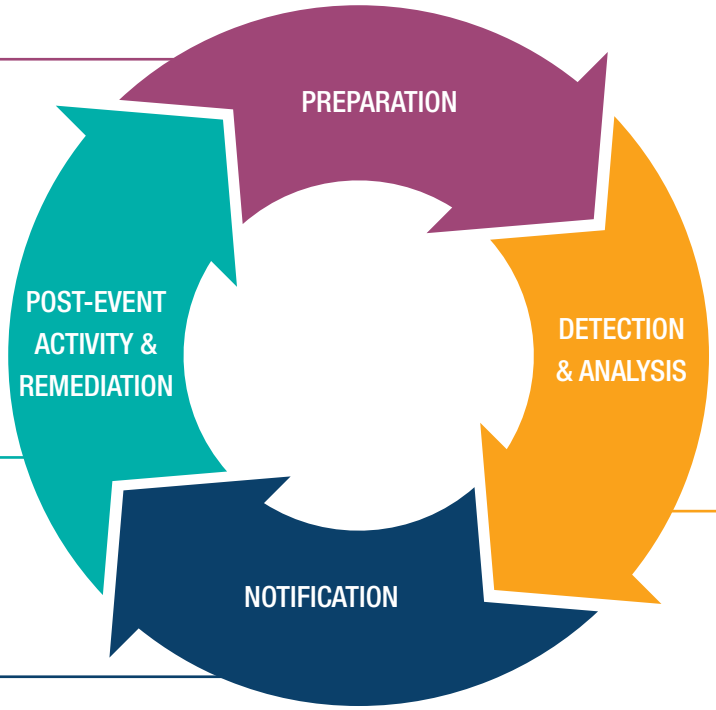
CYBERSECURITY
Our Service Approach

Industry recognized leaders

Our team of experts has extensive experience advising companies of all sizes across a wide spectrum of industries, including life sciences, healthcare, financial services, and technology companies. We have worked on a wide range of cybersecurity incidents, from simple business email compromise to elaborate cyber-extortion attacks against publicly traded companies. When any event occurs, our team provides end-to-end and around-the-clock advice on timing and sequencing of notifications. We advise clients on data security breach and incident response, responding to regulatory investigations (Federal Trade Commission, state Attorneys General, industry sector regulators, data protection authorities) and post-breach remediation, including class-action litigation defense and representation before data protection authorities and other government agencies.

Our Integrated Solution

- Pre-breach/ compliance services, refining processes and procedures, reviewing and drafting security incident response plans, and assisting with simulations
- Benchmarking against current industry practices and standards
- Integrated counsel on broader potential implications for reputation, criminal and civil litigation exposure and employees and investor relations that may flow from an incident
- Design and implement appropriate steps on remediation; demonstrate the credibility of those plans to regulators by reference to investigations data



- Develop proportionate strategies for investigating breaches and coordinate investigations across multiple regulators, including SEC
- Project manage the internal and external investigations teams, including third party providers
- Manage consequential litigation

- Coordinate regulatory reporting and notifications owed to affected individuals
- Assist companies through the various time sensitive stages of a data security breach investigation and stakeholder notification process
- Leverage experience and relationships of trust established with third party service providers and relevant industry regulators

- Advise on safeguarding and maintaining legal privilege around the investigation
- Provide support on engagement with media, government, shareholders, investors and customers – both in terms of identifying legal risk and in formulating appropriate messaging

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 have 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 helped a state department of occupational licensing to navigate a vulnerability in third-party software involving notification to approximately 600,000 individuals.

Ransomware Attack on Fortune 500

We helped 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.

Restoring Bank Operations After a Ransomware Attack

A Buchanan team led response efforts for a financial sector entity affected by a sophisticated ransomware attack that targeted over 100 banks and credit unions. We implemented remediation strategies to restore operations swiftly and enhance cybersecurity posture against future threats.

Partnering with the U.S. Secret Service to Mitigate Business Email Compromise

Buhanan managed a high-stakes investigation into business email compromise and wire fraud targeting a rapidly expanding company involved in frequent M&A activities. We worked in conjunction with the US Secret Service to trace and recover a significant portion of the misappropriated funds, safeguarding the company's financial integrity.

Crisis Management for a Multinational Healthcare Company

Provided crisis management and incident response assistance to a multinational healthcare company that had a breach involving several thousand O365 accounts and subsequent investigations. This matter was a true crisis situation, where the team mobilized to ensure best outcomes for the client, including coordination with incident response vendors, authorities, and other key stakeholders.

Malware Attack on a Global Healthcare Company

Served as lead outside cybersecurity-related legal advisor and investigations and crisis management counsel on a multi-country cyber extortion attack and subsequent investigations. This malware incident resulted in an operational impact on the company's ability to deliver IT services for an extended period. The team assisted the company in prioritizing which systems needed to be functional to reduce business interruption.

Our clients want lawyers with excellent technical skills who can look ahead to help them navigate a constantly changing world. It means having lawyers who can anticipate what is coming next and are comfortable with business level discussions

475
ATTORNEYS AND GOVERNMENT RELATIONS PROFESSIONALS

17
OFFICES

Other Core Practices:

Antitrust and Trade Regulation
Corporate Finance
Energy & Environmental
Government Relations & Public Policy
Healthcare
Immigration
Intellectual Property
International Trade & National Security
Labor & Employment
Litigation
Real Estate
Tax
Wealth & Succession Planning
White Collar Defense, Compliance & Investigations

Where some law firms stop at regulatory counsel, data protection and incident response, our holistic, 360-degree approach to data goes much further. Buchanan's integrated approach gives us a distinct advantage in helping clients prepare for and respond to ransomware events and other cybersecurity crises. With deep understanding of our clients' data assets, data flows, security protocols and optimization strategies, we develop tailored and effective response plans and crisis management materials in preparation for potential adverse data incidents. When the need arises, our full-service team will help with internal investigations, regulatory coordination, and navigating the legal and business issues in the wake of any event.

For additional information, contact our Cybersecurity & Data Privacy team or email us at cyber@bipc.com.

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

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

HARRY A. VALETK
Shareholder
harry.valetk@bipc.com
212 440 4416 | New York, NY

JENNIFER M. OLIVER
Shareholder
jennifer.oliver@bipc.com
619 685 1990 | San Diego, CA

KURT SANGER
Cybersecurity Counsel
kurt.sanger@bipc.com
813 222 1103 | Tampa, FL

ANDRIA ADIGWE
Associate
andria.adigwe@bipc.com
212 440 4409 | New York, NY

JACQUELINE V. JONCZYK
Associate
jacqueline.jonczyk@bipc.com
215 665 5319 | Philadelphia, PA

TIFFANY YEUNG
Associate
tiffany.yeung@bipc.com
215 665 3843 | Philadelphia, PA

BIPC.com/cybersecurity-and-data-protection