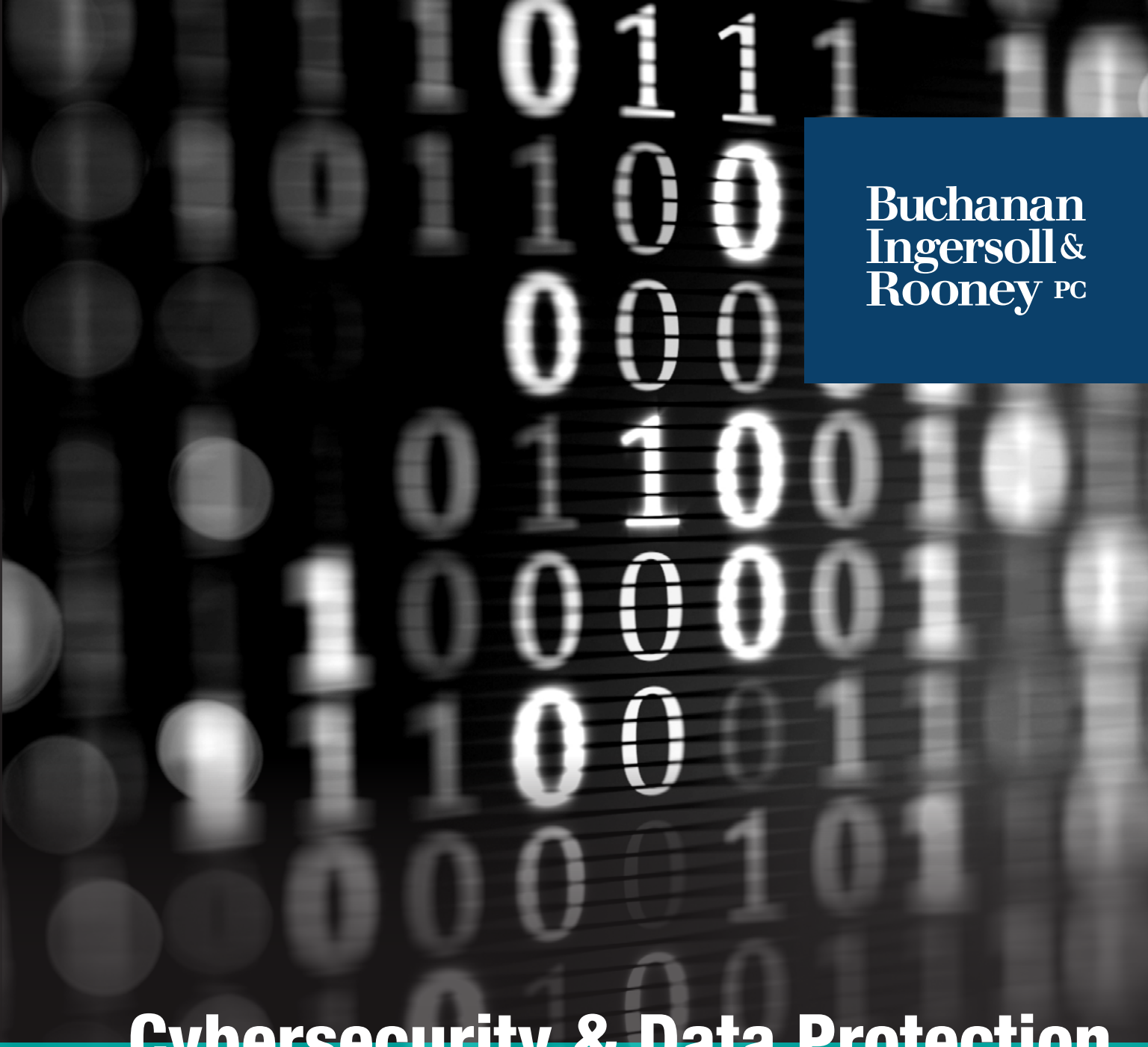


Buchanan Ingersoll & Rooney PC

# Cybersecurity & Data Protection

# Fielding Your Quarterback

Wherever your data resides, it's at risk. Having a seasoned quarterback on your team who knows the legal, regulatory and technical triad of cybersecurity can help you manage this complex playing field.

## How We Can Help You

### Ready to Defend You

If a breach occurs or you suspect one has, there's much to do. We will guide you through the intense process of investigation, analysis, and communications and, if necessary, defend you in government investigations and any litigation. Here's what you can expect:

**Working with Forensics.** An independent forensic investigation by an experienced information security expert is central to a breach response. We work with forensics experts to figure out what happened so we can advise you how to respond and how to meet legal and regulatory obligations while keeping the analysis as confidential as possible.

**Managing Internal Investigations.** Not all security breaches involve computers or hackers. An insider's accidental, negligent or intentional act can also cause a breach. Our team will investigate and provide the breach and employment law counseling.

**Need to Notify.** 48 states and multiple federal agencies have unique requirements for sending breach notification to affected individuals and regulators. While you work diligently to identify the affected individuals and their states of residence, we advise on the timing, content, and format required to meet your regulatory and contractual obligations.

**Right Message at the Right Time.** Breach response demands a well thought-out and centralized communications plan covering affected individuals, regulators, media and the general public. We will work with your communications team to centralize the process and your messages to mitigate adverse legal consequences and protect your company's reputation.

**In Your Defense.** When a cyber-incident results in an investigation by regulators or in private litigation, we can defend you in administrative investigations and proceedings and in court. We have advised clients through data breach and privacy class actions and individual plaintiff litigation, Department of Health and Human Services investigations, and interactions with other government regulators.

## Ready to Protect You

Developing and implementing a proactive data security program can seem daunting. But in today's world, doing so is critically important to meeting the legal standards of care. We can help you build a program to protect your organization's mission-critical information and the information entrusted to you by customers, employees and others.

**Crafting an Incident/Breach Response Plan.** Having an established plan in place before an incident occurs is significant to regulators. A tested plan improves decision-making and promotes coordination of critical functions, including IT, operations, legal and forensic experts, and internal and external communications.

**Training for Prevention and Response.** If properly trained, employees at all levels can be a major defense against phishing, hacking, and other cyberattacks. They will also know their role and priorities in responding to a breach.

**Conducting Tabletop Exercises.** Tabletop exercises simulate a real-time cyber incident and test the effectiveness of your security incident response planning and training.

**Establishing Relationship Protocols.** Because third-party access is a major threat for breaches, security regulators will scrutinize your third-party risk management. We can develop security protocols and contractual obligations for vendors and contractors with access to protected and other confidential information.

**Building the Program.** An effective information security program requires a joint effort by IT, HR, compliance, risk management and legal professionals. We will work with your team to build a program to address the rapidly evolving standards and expectations for enterprise security.

# Working with Clients Across Multiple Sectors

**Healthcare Providers | Educational 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**

# Advancing Our Clients' Goals

### Financial and Healthcare Institutions are Always High Risk

We helped a major regional bank and major hospital improve protocols for protecting customer and proprietary information, including developing enhanced employment and confidentiality agreements and privacy policies.

### Working with Government Entities

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.

### Helping Protect a Hospitality Business

A leading hospitality provider sought to protect itself with a comprehensive review and update of its security policies. Our team performed the review, suggested policy revisions, and provided customized data security training to managers and executives.

### Defense Following a Laptop Theft

On behalf of a healthcare automation solutions provider, we obtained dismissal of claims arising from the theft of an employee's laptop that contained protected health information. The dismissal was based on grounds that the court lacked subject matter jurisdiction because the plaintiff failed to adequately allege injury-in-fact.

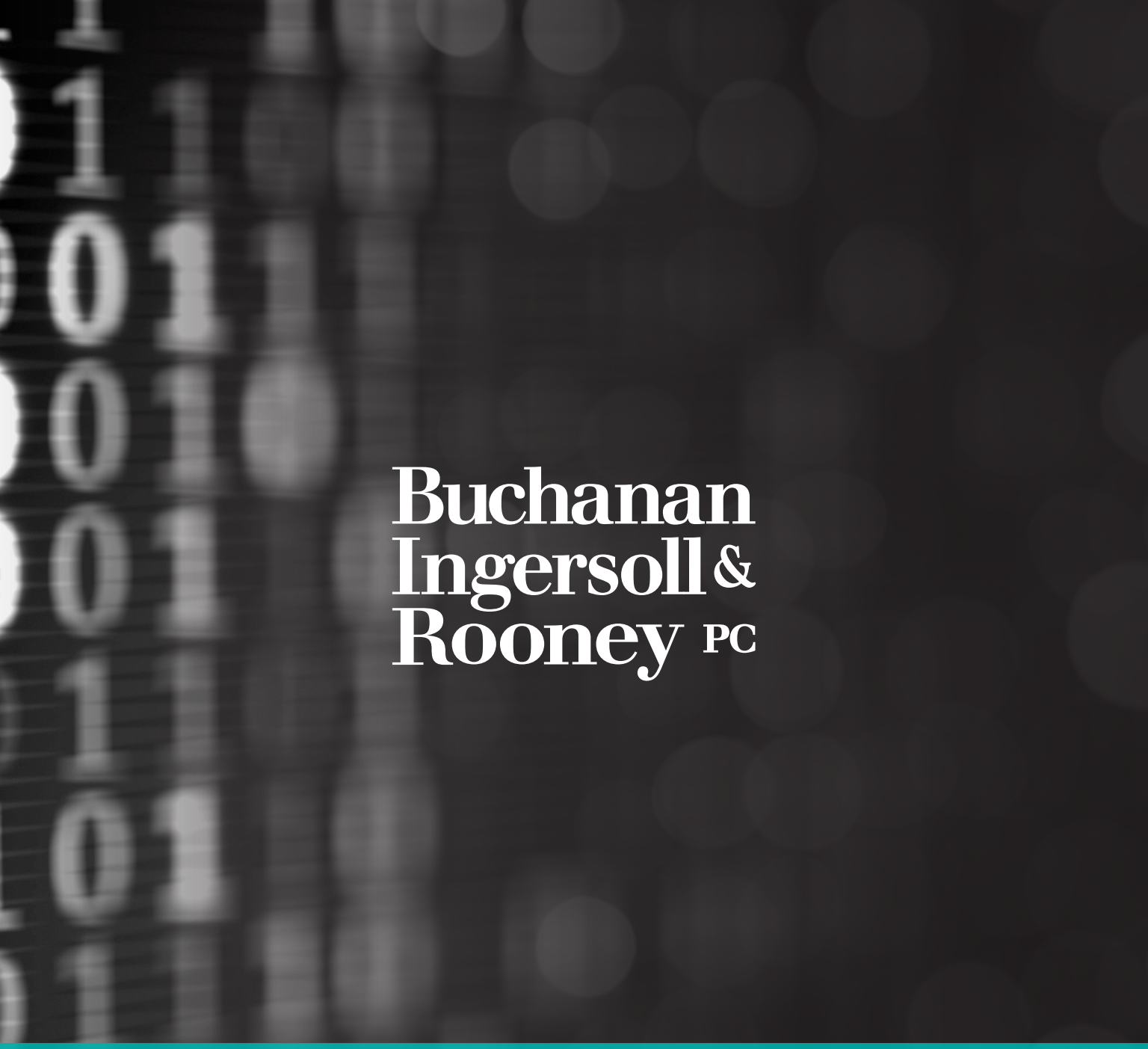
### Drafting a Game Plan to Avoid Future Risks

A national home builder and a community healthcare system enlisted our help with a potential data breach. An independent investigation concluded that protected information was most likely not breached. Our work didn't stop there. To prevent future risks, our team recommended an immediate assessment of their vendor management programs and contracts.

**Learn more at BIPC.com**

**Visit Buchanan BreachCoach® at eRiskHub.com/BIPC**

Your portal to cybersecurity information and updates



Buchanan Ingersoll & Rooney PC

BIPC.com