CYBERSECURITY AND DATA PRIVACY: ELECTRIC, WATER & WASTEWATER UTILITIES

NetDiligence AUTHORIZED BreachCoach

Protect. Prepare. Respond. Defend.

Protecting your data network means safeguarding the very core of your organization. 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 technical and operational systems.

In today's digital age, cybersecurity and data privacy have become critical concerns for electric, water and wastewater utilities. As these essential services increasingly rely on interconnected technologies and smart infrastructure, they face heightened risks from cyberattacks that can disrupt operations, compromise sensitive data, and undermine public trust. By prioritizing robust cybersecurity measures and data privacy practices, utilities can enhance their resilience against evolving threats, stay compliant with regulatory and contractual requirements, and ultimately ensure the reliable delivery of essential services to the communities they serve.

What We Do

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

Our extensive experience equips us with the ability to quickly identify the root cause of an issue, facilitate operations in a degraded information technology environment, provide immediate technical and legal advice, and forecast risks and liabilities that utilities might face in the future. Our security professionals conduct in-depth data analysis well in advance to identify potential vulnerabilities and threats, helping to inform legal strategy and decision-making.

Most importantly, our experience in responding to incidents uniquely positions us to help organizations prevent incidents. Having learned the lessons of multiple cybersecurity events, we understand how malicious hackers operate and leverage this knowledge to craft defensive security measures.

How We Can Help You

Incident Response Readiness and Compliance

Our approach involves working closely with you to develop, refine and document your cybersecurity programs and incident response plans. We collaborate with forensic and crisis communication experts to provide effective training for your response teams. By conducting cybersecurity tabletop exercises tailored to utilities, we simulate real-world, dynamic threat situations to evaluate organizational readiness and identify response plan gaps. In the event of an incident, our Cyber Response Team provides 24/7 support. Beyond legal advice, our team helps ensure your IT systems and processes comply with various legal requirements through technical audits and actionable improvement recommendations.

Digital Risk Advisory

We guide utilities through inquiries and assessments by local, state and federal agencies. If a security incident results in a lawsuit, we work closely with you 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 position your organization to prevent breaches. Recognizing that all systems are vulnerable, we also ensure your organization is breach-ready and resilient. Drawing from our vast experience and constant analysis of evolving cyber threats, we help enhance your operational framework by:

- Understanding the goals and dynamics of an organization to ensure the use of technology, and its protection, best supports achieving those goals
- Crafting risk-based security strategies, using key insights from our security partners and our internal technical expertise to provide comprehensive recommendations
- Undertaking "reasonable security" evaluations to defend against potential legal or 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
- Streamlining vendor management and technology contracts and brokering agreements involving advanced security technologies
- Establishing comprehensive cybersecurity risk management programs and collaborating with leadership at all levels. This includes setting up foundational security measures, charting cybersecurity roadmaps and gauging cybersecurity maturity

Privacy and Data Security Litigation

Cybersecurity breaches can have severe consequences for individuals and organizations. If a breach results in legal action, our litigation team is highly experienced in post-breach suits and will defend you in any form of litigation, including single-plaintiff lawsuits, class actions or actions brought by regulatory authorities.

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

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

JENNIFER M. OLIVER
Counsel
jennifer.oliver@bipc.com
619 685 1990

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

BIPC.com/cybersecurity-and-data-protection