Dickie McCamey
ATTORNEYS AT LAW

Cybersecurity

Managing Emerging Cybersecurity Risks and Challenges

In today's information technology-driven world, no company, industry or sector is immune from cybersecurity risks and attacks. Data breaches and other cybercrimes are not only on the rise, they are becoming increasingly more complex and challenging to manage. Everyone is vulnerable and must take proactive measures to protect their organizations from these far-reaching threats and attacks.

The attorneys at Dickie, McCamey & Chilcote help clients address the rapidly-evolving legal issues and challenges associated with cybersecurity risks and attacks. We know our clients' industries and work with them to implement strategies designed to manage data security threats specific to their businesses. When a data hack or other cybersecurity incident occurs, our attorneys take immediate action to help clients respond appropriately and protect their businesses from cybersecurity-related lawsuits and liability.

Counseling Clients on Cybersecurity Protection Measures

Dickie McCamey's cybersecurity practice focuses on helping organizations adopt preventative measures to protect data from cybersecurity breaches and attacks. Our lawyers shepherd clients through detailed data vulnerability analyses to identify potential security risks and threats within their organizations. We ensure that our clients are taking appropriate steps to comply with data security laws and regulations, including developing Business Associate Agreements (BAA) and meeting other requirements under the Health Insurance Portability and Accountability Act (HIPAA). We also advise clients on Federal Credit Reporting Act (FCRA) privacy standards and work with organizations to implement best practices for their Bring Your Own Device (BYOD) programs. Additionally, members of our practice assist clients in evaluating cybersecurity and other insurance policies designed to mitigate losses and liability stemming from security breaches and attacks.

Responding to Cybersecurity Incidents

When a cybersecurity incident occurs, the attorneys in our practice are fully prepared to help clients develop an appropriate plan of response. Our IT team acts quickly to determine the location of the breach, how long it has been occurring, and the scope of the data that has been compromised. We also implement targeted procedures to preserve and recover data and advise clients on applicable data breach notification statutes that may require notifications to state and federal agencies as well as individuals who may have been impacted by the breach.

The attorneys at our firm recognize that cybersecurity incidents can be extremely damaging to our clients' business reputations. Cyberattacks and threats are "hot" issues, and we take quick action to protect our clients from adverse media campaigns. When a breach turns into a lawsuit, we are prepared to protect our clients at every stage of the process. Our attorneys have handled cybersecurity cases of all sizes, ranging from individual lawsuits to massive customer and employee class action suits. In Pennsylvania, we represented a large health system in a class action lawsuit filed by employees whose personal information was stolen in a data breach. In this case of first impression, the trial judge ruled that the health system did not have a duty to protect the employee's personal information. This ruling was upheld on appeal to the Pennsylvania Superior Court and is currently being appealed to the Pennsylvania Supreme Court.

Our experience and understanding of the legal and technical issues involved in cybersecurity lawsuits gives our clients an added advantage when a cybersecurity incident surfaces. We are well-versed in computer systems and network operations and know the key experts in the field who can help us develop the strategies needed to successfully protect and defend our clients regardless of the size or scope of their case.