White and Williams LLP

Cyber Law and Data Protection

The Cybersecurity and Data Privacy group is comprised of a multidisciplinary team of highly qualified lawyers with intimate knowledge of the insurance industry and experienced in compliance, corporate governance, first and third-party coverage, and litigation.

Insurance carriers long have turned to White and Williams for advice. For cybersecurity and data privacy, it is no different. Our attorneys bring a deep breadth of experience in the insurance industry, and advise insurance carriers in a wide array of matters from compliance and corporate governance to first-party and third-party coverage matters, and litigation.

Compliance with Data Security and Privacy Laws and Regulations (Pre-Breach Services)

If your company has data, it's a target. Depending upon the industry, your company likely has legal requirements to develop and implement an adequate data security program to safeguard the confidentiality, integrity and availability of information and your company's information systems. Data security programs include written policies and procedures, documented employee training, vendor oversight, and sometimes personal certification of compliance with a cybersecurity law or regulation by a C-Suite officer.

White and Williams assists clients with developing and implementing comprehensive data security and privacy programs to meet their legal needs under growing state and federal data protection laws and regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HI-TECH Act), the Gramm-Leach-Bliley Act (GLBA), and the New York Department of Financial Services cyber regulations. We also help clients comply with the EU's General Data Protection Regulation (GDPR) as well as the California Consumer Privacy Act (CCPA). Our lawyers help clients draft policies and procedures, including incident response plans, respond to requests for certification of compliance from regulators and business partners, conduct training and tabletop exercises, and establish third-party vendor management programs.

Mergers, Acquisitions, and Corporation Disclosures

An entity's cybersecurity health is critical to its value in the context of a merger or sale. A prior cybersecurity incident or lax safeguards that fail to mitigate risk represent significant potential liability (and decreased value). White and Williams helps clients conduct the required and critical due diligence to assess and evaluate cybersecurity policies, programs, and incidents, whether they are the

PRACTICE CONTACTS

Paul A. Briganti, Counsel
215.864.6238
brigantip@whiteandwilliams.com

J. Christopher Erb, Counsel
215.864.7046
erbj@whiteandwilliams.com

RELATED PRACTICES

Commercial Litigation

Corporate and Securities

Cyber Subrogation

Healthcare

Insurance Coverage and Bad Faith

Intellectual Property

RELATED INDUSTRIES

Financial & Investment Services

Gaming

Healthcare

Insurance

Technology

subject of a potential sale and looking for fair value, or to provide an evaluation of risks a client may inherit through a transaction. Our lawyers also review technology contracts and transactions to strengthen our client's interests and protection.

Cybersecurity Incident Response and Notification

When an organization sustains a suspected cybersecurity incident they are required by law (or sometimes by contract, or both) to undertake a prompt investigation and provide notification of the incident in a short period of time. Sometimes, a company's notification window is a mere 72 hours after knowledge of the event. White and Williams provides clients with critical crisis management to investigate and respond to cybersecurity incidents. From ransomware to data breaches, our lawyers work with forensic investigators to determine the "who, what, why and how" of an incident. We help companies with coordinated public relations efforts, potential interactions with law enforcement, and determination of required third-party notifications to consumers, business partners, regulators, State Attorneys General, and others.

Litigation

A dispute involving a cybersecurity incident can devolve into litigation, whether a business-to-business lawsuit or a data breach class action. White and Williams represents corporations in a wide variety of business sectors in litigation in state and federal courts across the country. The firm's approach to complex litigation matters is to staff them with senior litigators who assemble efficient teams of attorneys.

Insurance

Insurance carriers long have turned to White and Williams for first-party and third-party coverage matters. For cyber liability, it is no different. Our lawyers provide exposure analysis and litigate complex coverage matters for cybersecurity incidents, from data breaches and business email compromises (BECs) to wrongful collection and use of personal identifiable information (PII), media liability, and e-surveillance. Our lawyers regularly write and lecture on insurance law, including on cyber and privacy insurance, and assist with policy drafting. White and Williams also offers in-house instruction and continuing education courses to insurance claims professionals on cyber liability and coverage issues.

REPRESENTATIVE MATTERS

Assisted with drafting and implementing information security programs under GDPR

Advised with compliance under New York DFS cyber regulations 23 NYCRR 500, including certification and implementation of cybersecurity programs

Led multiple investigations of cybersecurity incidents

Led and coordinated response effort to data breach suffered by corporate client, including coordination with law enforcement

Coordinated the investigation for an international corporation concerning internal and external fraud committed through its computer systems

Represented insurer in coverage matter involving high-profile security data breach

Coordinated and negotiated with law enforcement following contact with corporate client regarding potential data breach and identified theft ring involving former employee

Represented insurers in coverage litigation and related matters involving unlawful acquisition and use of PII

Helped client evaluate cybersecurity protocols, revise employee handbook for cybersecurity and privacy matters, and created in-house cyber response teams with corporate cybersecurity response plan

Advised client on compliance under NIST SP 800-171 Standard for DOD Contracting, including development and implementation of a cybersecurity program

Represented clients in response to government subpoenas for their electronic data

Counseled clients in addressing cyber-harassment issues

Drafted and updated online service agreements, privacy policies and terms of use for client's websites and intranet sites

NEWS

Christopher Erb Joins White and Williams as Counsel in Philadelphia
2.8.22

Congratulations 2020 DE, MA, NY and PA Super Lawyers and Rising Stars
11.5.20

Chambers USA 2020 Ranks White and Williams as a Leading Law Firm
4.23.20

13th Annual Coverage College Hosts Over 400 Insurance Professionals
11.1.19

Mike Kassak and Josh Mooney Reappointed as Vice-Chairs of American Bar Association's Cybersecurity and Data Privacy Committee
9.3.19

Chambers USA 2019 Ranks White and Williams as a Leading Law Firm
4.26.19

12th Annual Coverage College Features Current Trends and State of the Insurance Claims Industry
10.23.18

Mike Kassak and Josh Mooney Appointed Vice-Chairs of American Bar Association's Cybersecurity and Data Privacy Committee
9.4.18

Linda Perkins Joins White and Williams Philadelphia Office
2.1.17

Jay Shapiro Comments on Proposed Broadband Privacy Rules and Verizon Settlement
The Cybersecurity Law Report, 3.16.16

PUBLICATIONS

It's "Personal"– An Expansion of What Qualifies As "Personal Information" Under Pennsylvania's Data Breach Notification Law
Cyber Law and Data Protection, 12.6.22

Are Insurance Brokers the Next Target for Claims Arising From the Pandemic?
The Legal Intelligencer, 7.26.21

SCOTUS Decision on Autodialers Under TCPA Provides Handy Primer on Statutory Construction and Interpretation
Commercial Litigation Alert, 4.16.21

NYDFS Announces Cyber Insurance Risk Framework to Address Increasing Cyber Risk
Insurance Industry Alert, 2.5.21

Recent Case Impacts HIPAA and HITECH Act Penalties
Healthcare Industry Alert, 2.1.21

HITECH Act Amendment Offers New Incentive to Reduce Fines and Other Remedies
Cyber Law and Data Protection and Healthcare Alert, 1.8.21

HHS Proposes Significant HIPAA Privacy Rule Changes: Amendments Would Increase Individual and Institutional Access and Coordination of Care
Cyber Law and Data Protection and Healthcare Alert, 12.11.20

Between a Rock and a Hard Place: Advisories Target Ransomware Victims, Insurers
The Legal Intelligencer, 11.2.20

Federal Advisory Warns Hospitals Facing "Increased and Imminent" Cyber Threat; 400 Hospitals Already Targeted
Cyber Law and Data Protection and Healthcare Alert, 10.30.20

Return to Work: Guidance for Workplace Reopening
5.21.20

Threats, Opportunities Presented by New Technology in the Insurance Industry
The Legal Intelligencer, 8.6.19

Higher Ed Falls Victim to New Data Breach
Cyber News: Cyber Law News and Bytes, 4.3.19

Best Practices For Personal Data Security #DataPrivacyDay
Cyber News: Cyber Law News and Bytes, 1.28.19

Security of Critical Infrastructure Relies on Businesses to Build Resilience
Cyber News: Cyber Law News and Bytes, 10.25.18

Supreme Court Alert: The Government Must Obtain a Warrant for Cell-Site Records
Cyber News: Cyber Law News and Bytes, 6.22.18

CEO Zuckerberg: Facebook User Settings Protect Individual Data – Congress Is Not So Sure
Cyber News: Cyber Law News and Bytes, 4.13.18

Coalition of State Attorneys General Send Letter Demanding Answers from Facebook
Cyber News: Cyber Law News and Bytes, 3.28.18

United States v. Microsoft Raises Significant Questions Regarding Application of the Stored Communications Act
Cyber News: Cyber Law News and Bytes, 3.6.18

Washington Suburb Targeted by Cybercrime and Ransomware Attacks
Cyber News: Cyber Law News and Bytes, 3.1.18

How Employers Can Respond to the Equifax Breach
Cyber Law and Data Protection Alert, 9.25.17

UPDATE: U.S. DHS Issues Revised Alert on WannaCry Ransomware
New Alert Details Indicators Associated with Ransomware and Recommended Steps for Prevention and Remediation
Cyber Law and Data Protection Alert, 5.15.17

Critical Security Updates Released by Leading Software and Technology Companies
Cyber Law and Data Protection Alert, 4.20.17

Department of Homeland Security Issues Internet Security Alert Ahead of Easter Holiday
Cyber Law and Data Protection Alert, 4.13.17

Reasonable Expectations of Privacy in a Not-So-Private Electronic World
Westlaw Journal Computer & Internet, 4.22.16

U.S. Department of Health and Human Services Issues New "Guidance" on Mobile Health Applications
Healthcare Alert, 3.18.16

FCC Issues Proposed Privacy Rules Applicable to Broadband Internet Service Providers
Cyber Law and Data Protection Alert, 3.11.16

Hospital Pays Ransom to Hacker in Response to Malware Attack: An Eye-Opening Reality
Cyber Law and Data Protection Alert, 3.9.16

The Supreme Court Upholds a Cyber Trespass Conviction
Cyber Law and Data Protection Alert, 1.26.16

Administrative Law Judge Rules Against FTC in Data Security Enforcement Action
Cyber Law and Data Protection Alert, 11.19.15

Creating a Culture of Cybersecurity in the Workplace
Cyber Law and Data Protection Alert, 10.9.15

Securing Electronic Medical Records on Mobile Devices
Healthcare Alert, 8.26.15

Full House To Begin Debate On Data Security and Breach Notification Act After Approval Of Energy and Commerce Committee
Cyber Law and Data Protection Alert, 4.16.15

EVENTS

COVID-19 Insurance Program
Webinar, 8.11.20

Creating a Data Privacy Compliance Program on a Limited Budget
Gallagher's Cyber Insight Series (Webinar), 7.22.20

Electronic Information in Criminal Investigations and Proceedings
American Bar Association (New York, NY), 1.13.20

ACC: Annual Ethics & Diversity CLE
ACC (IBM, North Castle, NY), 10.24.19

Electronic Information in Criminal Investigations & Proceedings
American Bar Association Webinar, 7.8.19

2019 Lehigh Valley Employment Law Seminar
National Museum of Industrial History (Bethlehem, PA), 6.5.19

Electronic Information in Criminal Investigations & Proceedings
New York State Bar Association (New York, NY), 3.13.19

Policy, Deals and Disclosure: A Lawyer's Role in Managing Security and Data
ACC Westchester/SCT (Purchase, NY), 6.12.18

2017 NAIC Insurance Data Security Model Law
New Reporting Rules Following a Cybersecurity Breach
Strafford Webinar, 3.29.18

The Implications of Cross-Border Discovery on Cybersecurity and Privacy Compliance
2017 Philadelphia Bench-Bar Annual Conference (Atlantic City, NJ), 10.13.17

Beat the Breach: Cyber and Data Protection and Regulatory Compliance
Philadelphia, PA, 10.11.17

Employment Law Seminar - Philadelphia
Philadelphia, PA, 4.12.17

Employment Law Seminar - Lehigh Valley
Penn State Lehigh Valley (Center Valley, PA), 6.9.16

Managing Cybersecurity in the Healthcare Industry: Best Practices Every Healthcare Organization Needs to Know
The Knowledge Group Webinar, 5.3.16

Cyber Risk and Cyber Insurance - What You May Know and May Not Know
Association of Corporate Counsel (Westchester/Southern Connecticut Chapter), 1.22.16

Cybersecurity Panel Discussion
Brooklyn Chamber of Commerce (Brooklyn, NY), 1.18.16

Finance Forum: Cybersecurity in Financial Transactions
Philadelphia, PA, 11.12.15

Ethical Issues Facing In-House Counsel Today: Data Breaches, Confidentiality and Compliance
Association of Corporate Counsel, Westchester County NY/Southern Connecticut Chapter, 11.6.15

Employment Law Seminar
Philadelphia, PA, 5.20.15

Healthcare and Data Breaches - Vulnerability and Consequences
2015 Healthcare Summit, 5.7.15