POLSINELLI

Kayleigh S. Shuler

ASSOCIATE

Kansas City, MO | 816.360.4181
kshuler@polsinelli.com

Kayleigh and her colleagues often say it is not a matter of “if” but “when” a company will find itself responding to a possible data breach. To help clients prepare and respond effectively, Kayleigh provides guidance before, during, and after incidents.

During a security incident, Kayleigh helps clients create a game plan for investigating what happened and resolving any operational or communication challenges. If there are potential obligations to notify employees, other individuals, customers, law enforcement, or regulatory bodies, Kayleigh helps clients identify and meet those obligations. If attorneys general, law enforcement, or other government agencies demand more information, Kayleigh helps clients respond strategically. The types of incidents that Kayleigh advises on include:

- Ransomware
- Phishing, spam attacks, wire fraud, and other email-related compromises
- Inadvertently disclosed documents
- Lost or stolen devices
- IT scams
- Employee wrongdoing
- Incidents occurring at vendors and other third parties

Before and after an incident, Kayleigh helps clients plan for the future, with an eye toward reducing the frequency of incidents and the scope of their damage. Her pre- and post-breach services include:

- Educating boards of directors and other stakeholders on cybersecurity preparedness
- Conducting tabletop exercises to “dry run” who would do what during an incident
- Developing (or improving existing) policies on:
    - Incident Response Protocols
    - Document Retention
    - Employee Cyber Awareness and Training
    - Employee Use of Company and Personal Devices

In all of these matters, Kayleigh is well versed in the particular needs of clients in sectors

Capabilities

- Technology Transactions
- Privacy & Cybersecurity
- Information Security (InfoSec)
- Data Breach & Incident Response
- Financial Institutions Privacy
- Technology

like: education; banking, credit unions, and other financial services; manufacturing; health care; technology; retail; and municipalities and other governmental entities.

Education

- University of Oregon (J.D., *Order of the Coif*, 2016)
    - Executive Editor of Oregon International Law Review
- Missouri State University (B.S., *summa cum laude*, 2013)

Bar Admissions

- Missouri, 2020
- Oregon, 2016

Publications

June 2024
It's Not Your Fault, But It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks
Author, The Banking Law Journal Vol 141 No 6

January 24, 2024
2024 Tech Transactions & Data Privacy Report

January 24, 2024
It's Not Your Fault, but It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks

September, 2023
The Increasing Risks and Prohibitions Associated With Paying a Ransom After a Ransomware Attack
The Computer & Internet Lawyer

May 16, 2023
Institutions Subject to FTC's Enacting Regulations to GLBA Must Implement Information Security Programs by June 9, 2023

March 30, 2023
The Increasing Risks and Prohibitions Associated With Paying a Ransom After a Ransomware Attack

February 2, 2023
Tech Transactions & Data Privacy 2023 Report

December 6, 2022
How Health Care Professionals Can Limit Their Liability Following a Cyber Attack
Co-Author, AHLA

February 2022
Tech Transactions & Data Privacy 2022 Report

September 23, 2021
Department of the Treasury Issues New Advisory Regarding Ransomware Payments

February 23, 2021
Cyber Incident Response Plans – Turning Words into Action
Co-Author, 4Hoteliers

January 25, 2021
Tech Transactions & Data Privacy Report