Data Security Counseling/Data Security Audits

Overview

Our group counsels clients regarding state, federal and international data protection and privacy laws. Although every business has legal obligations in this area, we also offer counsel with regard to industry-specific laws and regulations, including, among others, the California Consumer Privacy Act, Payment Card Industry Data Security Standard (PCI DSS), Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), Electronic Communications Privacy Act, Children's Online Privacy Protection Act, Fair Credit Reporting Act, Federal Trade Commission Act, and Sarbanes-Oxley.

In providing data security counseling, we address the legal requirements applicable to the individual business and assess the legal risks associated with each client's business and practices.

We also:

- Manage cyber risk assessments and data security audits
- Help develop incident response plans
- Oversee "penetration testing"
- Develop and document policies and procedures that address privacy and information security, such as:

  - Data management (identification, classification, retention, and destruction of data)
  - Business continuity and disaster recovery
  - Monitoring (including audit logs, system events, security events, personnel and external service providers)
  - Removable media protection and restrictions
  - Anti-virus/anti-malware software
  - Patch/upgrade management
  - Remote access restriction

Primary Contacts

Mark J. Sever, Jr.

Partner

msever@archerlaw.com

856.354.3045

Kate A. Sherlock

Partner

ksherlock@archerlaw.com

856.673.3919

Christian A. Stueben

Partner

cstueben@archerlaw.com

201.498.8512