Business Case

- Mitigate company regulatory, legal, financial and reputation risks, and loss of productivity due to a breach.
- Protect customers and employees from financial, medical, and reputation risks associated with identity theft.
- Protect company intellectual property and trade secrets and infrastructure and technology from compromise and business disruption.
- Enable business development, M&A and investment opportunities.
- Protect executives and directors from D&O class action lawsuits and job loss.

Presumption of a Breach

Regulatory guidance advises that organizations must presume they will suffer a breach. Unfortunately, compromised organizations learn the hard way that **check-the-box compliance does not establish a legally defensible posture**. This means that in addition to the direct costs of a breach, you are exposed to additional legal costs, regulatory fines and burdening oversight, such as a 20 year FTC consent order or a 3 year HHS resolution agreement. While legitimate issues, budget and resource impacts cannot be used to legally justify inaction or inadequate controls to a regulator or plaintiff lawyer. Organizations need to systematically and continuously identify foreseeable risks and apply reasonable standards of care to be in a legally defensible posture.

Value Proposition

SoCal Privacy helps public and private organizations establish a lean, sustainable, legally defensible security and privacy program, including appropriate data governance with clear roles and responsibilities. We work with you to develop data flow maps, inventories, and locations, and use these to help you identify foreseeable risks. These risks are then assessed, controls evaluated for effectiveness, and, where appropriate, mitigation plans developed to improve the strength of controls. We categorize data into sensitivity levels using a risk management approach, and help you develop scalable strategies, policies and procedures that match the strength of controls to the data sensitivity level, such as for an enterprise cloud use case strategy. As another example, service provider requirements for due diligence, agreement's reps and warranties, and periodic monitoring will be based on data sensitivity levels.

Contact Us

SoCal Privacy Consultants
754 Banyan Court
San Marcos, CA 92069

Phone: 619-318-1263
Fax: 760-946-7824

info@socalprivacy.com
www.socalprivacy.com

SoCal Privacy Consultants
Lean. Sustainable. Legally Defensible.

SoCal Privacy Consultants

Who We Are

Lean

We develop strategies to right-size our clients' privacy and security programs based on organizational size, complexity, objectives, risk profile, and risk tolerance.

Sustainable

We help clients establish effective and scalable governance with clear roles and responsibilities to continually sustain their organization's privacy and security program.

Legally Defensible

We help clients develop and implement a risk management approach to identify foreseeable risks and apply reasonable standards of care to create a legally defensible posture.

Services

Privacy and Security Gap Assessment

- For companies / subsidiaries, M&A buyers / sellers
- Policies and procedures review
- Data flow, inventory and locations mapping
- Controls evaluation to standards
- Risk assessment
- Strategic plan
- Findings and recommendations report

Privacy and Security Program Establishment

- Design governance infrastructure / roles and responsibilities
- Define risk management and controls framework
- Develop policies / procedures
- Develop / deliver training
- Design program monitoring

Vendor Management

- Vendor privacy / security due diligence
- Vendor privacy / security contract requirements
- Cloud services (use cases) policy / guidance
- Cloud / collocation hosting service provider due diligence
- Managed security services – build vs. buy guidance / assessment
- Vendor management program / policy: due diligence, contracting and monitoring

Privacy / Security-by-Design

- Privacy engineering (SDLC) policy & training
- Privacy requirements, controls, & design

Support Hiring and Development

- Source / interview CPO / CISO candidates
- Train / mentor internal candidates

Incident / Breach Investigation and Response

- Incident / breach investigation and response guidance and policies
- Identify third party breach support vendors
- Coordinate incident / breach investigation and response

More Services

Consulting Services - a la carte

- Obtain executive commitment
- Data flow, inventory and locations mapping
- Privacy / security strategic plan
- Comprehensive controls evaluation
- Risk assessment
- Develop policies / procedures, e.g. acceptable use policy
- Develop / deliver training
- Cross border transfer rules guidance
- SEC cyber risk disclosure guidance
- Workplace & social media privacy guidance
- Audit preparation

Standards and Controls We May Use to Assess Your Privacy and Security Posture

- Council of Cybersecurity's Top 20 Critical Security Controls
- HIPAA / HITECH
- NIST Cybersecurity Framework
- ISO/IEC 27002:2013
- PCI-DSS v3.0
- SEC OCIE Cybersecurity Initiative
- GAPP (Generally Accepted Privacy Principles)
- U.S. Sentencing Guidelines for Effective Compliance Programs

SoCal Privacy Consultants

Lean. Sustainable. Legally Defensible.

Certifications

Certified Information Privacy Professional
CIPP

Certified Information Systems Security Professional
CISSP

Certified Information Systems Security Professional

Certificate of Cloud Security Knowledge
CCSK

Certificate of Cloud Security Knowledge

Affiliations

International Association of Privacy Professionals
IAPP

iapp
international association of privacy professionals

International Information Systems Security Certifications Consortium
(ISC)²

Cloud Security Alliance
CSA

cloud security alliance®

Testimonials:
www.socalprivacy.com/testimonials