Data Security and Privacy for Board Members

Minimize Risk, Reduce Cost, Protect the Board of Directors

Version 1.4

July 8, 2020

info@assuredSPC.com

Assured SPC

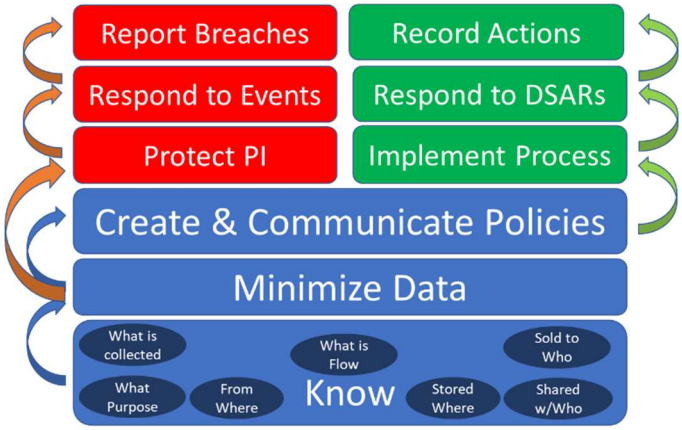
Privacy does not have to be complicated. Many organizations create significant financial and reputational risk for themselves through decisions on governance, cultural change and adoption of regulatory compliance requirements for consumer privacy. If the early steps of privacy compliance are done well and there is continuous focus on quality and automation, then risk and operational cost can be reduced -- and the fiduciary responsibilities of the board of directors can be satisfied.

Regulatory requirements

There are many country and state laws enacted to protect personal information. There are a cornucopia of these laws including, but not limited to the General Data Protection Regulation (GDPR), the Health Information Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), the California Consumer Privacy Act (CCPA), and the Illinois Biometric Privacy Information Act (BPIA). Every US state and territory has a Data Breach law regarding loss of control of personal and sensitive information. The goal of each of these laws is to protect consumer or resident personal information. The location of an organization does not determine whether the organization is covered by a regulation. The residence of the person dictates this. So even collecting marketing data about consumers from other states can determine whether an organization is required to protect that person's information. The international nature of ecommerce is a significant contributor to compliance risk. The regulations create financial and reputational risk to the organization and a fiduciary responsibility of the Board of Director. Every privacy regulation includes regulatory fines for non-compliance and in some cases a private right of action for consumers or residents.

What's included in Privacy regulations?

Privacy regulations always include a foundational requirement for organizations to **KNOW** the why, what, where and with whom of personal information that is collected and shared. It is always smart, and sometimes required, to **MINIMIZE** the collection and retention of personal information to the amount needed for business and legal requirements. Organizations are always required to **PROTECT** the personal information and to **REPORT** breaches – loss of control of personal information. Robust privacy regulations require that organizations **RESPOND** to such security events and to respond to consumer or resident requests defined in the law. And if organizations respond to consumer/resident requests, they are often required to **RECORD** that they complied with these requests. We call this the Privacy Life Cycle Stack. The life cycle starts at the bottom and each layer is critical to operationalizing compliance.



Who are the Organizational Stakeholders of Privacy?

The core of privacy is personal information. Protection of personal information is a shared responsibility in the organization. There is a life cycle of personal information that is collected and managed by organizations. The life cycle contains a planning, collection and use phases.

- The Marketing Group is a stakeholder and is often the owner of these phases of the life cycle for personal information that is not personal health information.
- The Information Technology group is a stakeholder because it can protect personal information that is stored in business systems.
- Human Resources and Payroll share the responsibility to protect employee personal information.
- Legal is accountable to informing other stakeholders about regulatory and contractual compliance requirements and to ensure that downstream compliance requirements are included in agreements with service providers and other third parties. The legal team is also accountable to create internal and external policies.
- Employees are stakeholders if they place personal information in documents or spreadsheets.
- Executive management is responsible for ensuring there is privacy governance

Privacy is not just an information technology issue. It is an organizational issue and therefore the board of directors has a fiduciary responsibility for privacy is heightened.

Operationalizing Data Security and Privacy

Effective implementation of data security and privacy programs is done by implementing each of the levels of the Privacy Lifecycle stack with a governance overlay delivered by the Data Privacy Officer (DPO) and the Chief Information Security Officer (CISO).

Efficient implementation of data security and privacy programs leverages automation to reduce cost in every level of the stack except for the level "Create and Communicate Policies". The next blog post will describe how automation reduces cost.

The Top 4 Data Security and Privacy organizational mistakes

We've seen 7 significant mistakes that organizations make that increase risk or cost of Data Security and Privacy programs. Here are the top 4:

1. **Lack of action** – Privacy laws continue to evolve and get adopted but today and at every day in the future privacy compliance is already law. Waiting for the California Privacy Rights Act on the November initiative or waiting for the Washington State privacy law or the next iteration of the NY State SHIELD act is risky. Privacy programs will need to be modified over time but the risk to the organization for not protecting personal information exists today.
2. **Not automating data mapping** – Many organizations think KNOWing where personal information is stored, why it is collected, who it is shared with needs can be done once. Marketing initiatives and other business operational systems will continue to change. Data mapping must be continuously updated. It needs to be part of the change process and automated to ensure completeness.
3. **Not minimizing data** – Just as records destruction activities based on records retention policies protect the organization, the same is true for personal information. If it isn't needed, don't collect it and don't store it longer than needed.
4. **Not automating the DSR procedure** - Most organizations have not automated the Data Subject Rights procedure. This not only affects quality of responses; it also has significant impact on the cost of each request.

Best Practices to Protect the Board and Reduce Cost

Privacy and Data Security need to be driven from the board and the C-suite. The financial and reputation risk is high for the organization – It is a best practice to include Privacy and Data Security in organizational risk management.

Privacy and Cybersecurity should be managed centrally to ensure that procedures, organizational responsibilities are clear and appropriate technology automation is used to control data security and privacy – It is a best practice to Create roles equivalent to the Data Privacy Officer (DPO) and Chief Information Security Officer (CISO). These can be fractional roles and outsourced for some organizations. These roles should provide regular reports to the privacy/security/IT sub-committees of the board.

Digital products and marketing programs need continuous change to respond to opportunities and marketplace changes. These will require changes to what personal information is collected. Update the knowledgebase/data map of changes continuously. Each step of the privacy life cycle stack should be done early and continuously improved to minimize risk to the organization, reduce ongoing cost and to protect the board of directors.

About Assured SPC

Assured SPC has expertise in the lifecycle of information security and privacy programs. We assist organizations with requirements for compliance including HIPAA, NIST, the California Consumer Privacy Act and the NY SHIELD Act to implement reasonable security procedures and practices and to implement the requirements and objectives of security objectives and privacy laws.

In addition to credentials and years of experience driving information security and privacy programs, Assured SPC's senior staff have deep experience as IT Leaders. We regularly help organizations prepare for AICPA SOC2 audits and HITRUST CSF assessments. We also offer virtual c-level leadership for SMB businesses, including Chief Information Security Officers (vCISO), Chief Information Officer (vCIO) and Privacy Officer services.

info@assuredSPC.com