Data Protection

Cisco program and framework

Overview

Protecting data is a mandate in today's global economy. With customers all over the world, organizations need to be able to demonstrate transparently how they are protecting data and ensuring privacy to earn the trust of their customers, users, partners and employees.

First and foremost, organizations need to build multidisciplinary teams. For data protection practices to be adopted, it's critical they seamlessly align with the operations of the organization. Privacy and Security teams need to lead the way together, but also need to bring in expertise and diverse perspectives from other teams.

Second, organizations need to inventory their data. You can't protect what you don't know that you have. Begin with a high-level exploration and work towards a more detailed data landscape. In all cases, seek to understand what data the organization has, where it is stored, who has access to it and from where, and how that data moves around the organization.

Protecting data globally: A modern mandate

Data is the currency of the knowledge economy. This makes it a highly valuable commodity – for organizations and cybercriminals alike. As threats to data security mount, organizations must find ways to keep their critical digital assets safe at all touch points and compliant to international data protection regulations that vary by country.

In parallel, choose a data protection program framework to use as the foundation for the program. There are many excellent options from which to choose. Organizations don't need to start from scratch, but they do need to adapt the framework to the culture and operational practices. Cisco's program includes:

- Policies and standards
- Identification and classification
- Data risk and organizational maturity
- Incident response
- Oversight and enforcement
- Privacy and security
- Awareness and education

With a framework established, organizations can gather best practices that deliver on core elements, adapting only as necessary for scale.

Next, assess organizational and data-centric risk. We also look at each data set and the opportunities it offers and the threats it faces across the organization and the ecosystem. Use the results of this risk assessment to focus your efforts. Start by taking action in the areas of greatest impact – positive or negative.

Finally, plan to iterate. Given the dynamic nature of the political and technology landscapes, you need to be agile. Begin with a minimum viable program and rapidly add sophistication over time.

Cisco's Data Protection Program (DPP) allows us to focus and respond effectively in an incredibly complex and dynamic environment by taking a collaborative, risk-based approach to data protection.

The following is Cisco's Data Protection Framework from our Data Protection Program (DPP).

Framework

Policies and standards

Policies and standards – common taxonomy, policy framework and core security, data protection and privacy policies.

Steps to start your policies and standards

1. Establish Common Data Taxonomy to Include:
   - Types of Data
   - Levels of Access
   - Data Related Roles
2. Create set of written standards, policies, and procedures

Standardized approach to industry certification and regulatory compliance

- Establish common data taxonomy
- Reconcile data standards, policies and procedures
- Align and assign data roles and responsibilities
- Determine accountability and decision rights

Framework

Identification and classification

Identification and classification – an inventory of our data and a map of our data landscape, letting us know what we have, where it is, where it flows, and who has access to it.

Data inventory

In order to know what to protect, you need to start by understanding what you have. An inventory, even if high level, can significantly improve your position.

- Identify structured and unstructured data
- Assess criticality to enterprise and customers
- Understand legal and regulatory obligations
- Maintain inventory and consistent classification

Oversight and enforcement

Oversight and enforcement – internal governance of the program, which includes monitoring adherence to policy, remediation, third party vendor management, and when requested, engagement with our board of directors.

Steps for success:

1. Monitor compliance enforce consistently
2. Develop oversight of third party data protection
3. Initiate proactive auditing and reporting
4. Enable corporate governance

Data risk and organizational maturity

Data risk and organizational maturity – both essential for a strong data protection and privacy program.

Data Risk Assessments help organizations understand where they show weakness in data security and personal privacy.

Maturity Assessments allow organizations improve data protection practices by looking at current strengths and weaknesses in relation to a set of data risk principles.

Framework

Incident response

Incident response – an enterprise-wide, data incident response process that's integrated with business continuity processes. This amounts to a virtual team that is ready to respond to data incidents leveraging a playbook with clearly outlined contacts and roles and responsibilities.

Incident response should include:

- Enterprise-wide data Incident Response Process (IRP) that is the integrated with corporate incident response program
- Process for taking corrective action where needed to uphold established data protection standards
- Expanded IRP to cover international requirements
- Enable cooperation with third party and customer IRPs
- Develop closed-loop corrective action process

Awareness and education

Awareness and education – change management and communication designed to create a security and privacy savvy culture.

Should include:

- Effective training, practical documentation and awareness programs
- Development, delivery and maintenance of collateral needed to educate the workforce, customers, and third party partners
- Build a network of advocates across the enterprise, partner to implement change and ensure adoption of new