ETHICO CYBERSECURITY & DATA PROTECTION

ESTABLISHING A DATA CLASSIFICATION SCHEME: KEY STEPS

Recent high-profile data breaches like Equifax have highlighted the risks posed when sensitive information is not properly classified and protected. Without rigorous data classification, companies may struggle to secure confidential data and ensure compliance with privacy regulations. A strong data classification scheme identifies sensitive assets, assigns categories and controls, and embeds policies into workflows. By proactively classifying and governing all data types, organizations can reduce breach risks and avoid regulatory penalties.

DEFINING DATA CLASSIFICATION

Data classification is the process of categorizing data by its level of sensitivity and value to guide appropriate security measures. This includes information like customer data, employee records, financial information, intellectual property, and other regulated or confidential assets. Common classification types include:

- Personally Identifiable Information (PII): Data tied to an individual such as name, address, SSN, financial details, medical history etc.
- Protected Health Information (PHI): PII related to an individual's medical records and health status.
- Financial Data: Information like credit card numbers, bank account details, and financial transaction records.
- Confidential Business Data: Trade secrets, intellectual property, pricing, corporate strategy and other proprietary information.

STEPS TO ESTABLISH A DATA CLASSIFICATION SCHEME

Creating and implementing an effective data classification framework involves **these key steps:**

IDENTIFY DATA TYPES AND SOURCES

Catalog all systems and databases containing sensitive data. This provides an inventory to classify. Document where regulated information like PII and PHI originate and flows between systems. Smaller companies don't need sophisticated software to engage in this process; an Excel spreadsheet will suffice.

ANALYZE VALUE AND PRIVACY IMPACTS

Evaluate the sensitivity level and potential impact of unauthorized disclosure for each data type, considering criteria like legal obligations, monetary value, damage to reputation or competitive advantage. Consider this from the perspective of your customers or key stakeholders: what information do you hold about them that would be most detrimental if it were subject to a security breach?

DEFINE CLASSIFICATION TIERS

Establish categories like "public," "internal," "confidential" and "highly confidential" with increasing levels of security controls at the internal level. Balance usability with protection.

STEPS TO ESTABLISH A DATA CLASSIFICATION SCHEME (CON'T).

DETERMINE CONTROLS

Specify appropriate access restrictions, encryption standards, retention rules, and other controls tied to each classification tier. Confidential data may mandate tighter access controls and encryption versus public data. As noted above, balance usability with protection. For example, if the customer service team occasionally needs to access categories labeled "highly confidential," then consider limited such access to 1-2 members on the customer service team who are at a senior level and have undergone specialized security and/or privacy training.

DOCUMENT POLICIES AND PROCEDURES

Formalize the scheme, controls per category, governance policies, procedures for classification, auditing requirements, and responsibilities in a data classification program document. These documents should be periodically reviewed to ensure that they are up-to-date with best practices and accurately reflect the operations within the organization.

BEST PRACTICES

Implementing an effective data classification approach requires:

- Cross-functional collaboration with legal, compliance, IT, security teams and business unit stakeholders.
- Leveraging common regulatory and industry frameworks like the Payment Card Industry Data Security Standard (PCI DSS) , Health Insurance Portability and Accountability Act (HIPAA), and Internal Standard Organization (ISO) standards.
- Considering third-party data risk by classifying vendor-accessed data.
- Balancing business needs through simple scheme and classification procedures.

IMPLEMENTING THE SCHEME

Once defined, the scheme must be implemented across systems including:

- Adding classifications to databases, file shares, applications to tag data at the source.
- Training employees on classification policies and their responsibilities.
- Building controls into workflows like automated data masking for test environments.
- Developing data handling procedures aligned to classifications like encryption and access reviews.

MAINTAINING COMPLIANCE

Ongoing governance ensures the program remains effective through:

- Periodic re-evaluation of classifications and controls against new regulations and risks.
- Regular audits to validate proper assignments and implementation of controls.
- Awareness training and policy attestation to embed classification practices.
- Issue escalation and remediation when errors or policy violations occur.

FINAL THOUGHTS

Data breaches often occur because sensitive information lacks proper safeguards. A data classification scheme tailored to regulatory and business requirements provides the foundation for strong data security and governance. The time investment to classify, protect, and govern data is minor compared to the fallout of compromised confidential information. Organizations that embrace proactive data classification reap benefits in compliance, consumer trust, risk reduction, and enabling data usage. By assessing your data landscape and needs, establishing tiers and controls, training employees, and embedding classification into workflows, you can unlock data's value while keeping it protected.

Contact Us for More Information | 800-859-8840
sales@ethico.com | www.ethico.com