Checking All Your Data Assets… Where Are They?

The Trust Bridge Virtual Conference

April 14th, 2020

Jody R. Westby, Esq.
CEO, Global Cyber Risk LLC

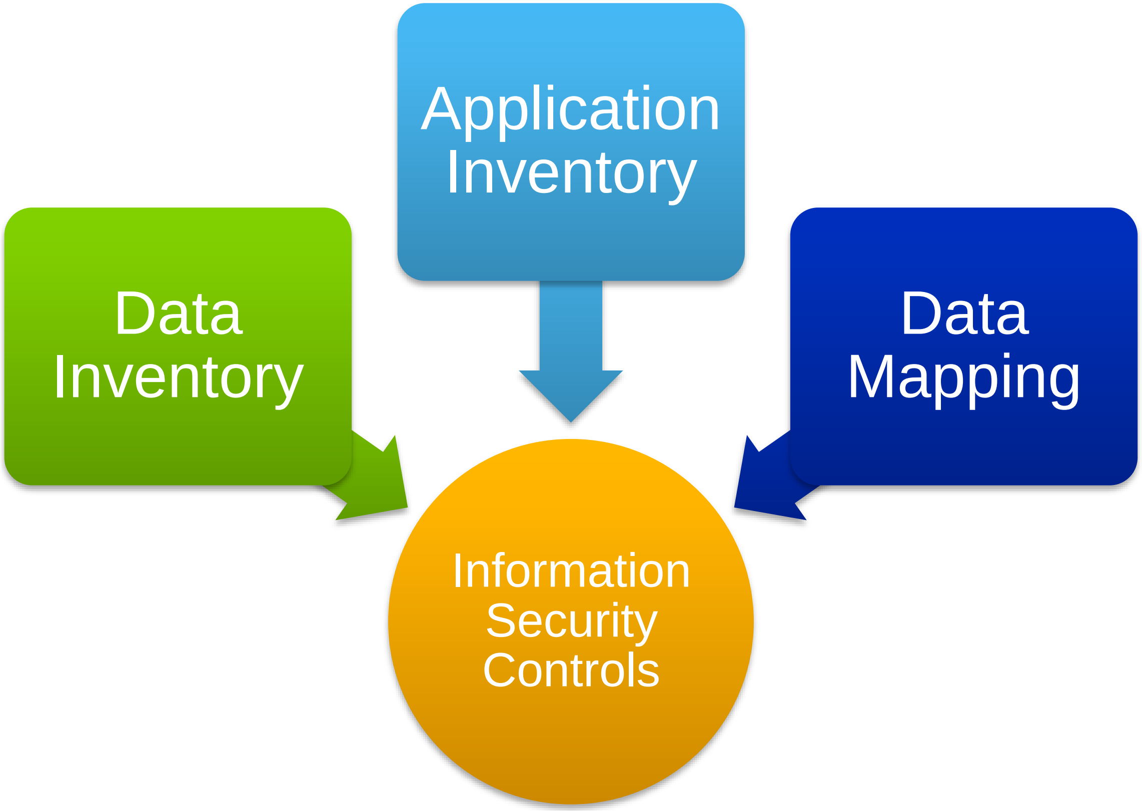
Why It Is Important to Know Your Data

- Foundation of data protection and cybersecurity programs -- Links them
- Required by data protection and cybersecurity best practices and standards
- Requirement of data protection and cybersecurity laws and regulations
- Data is essential to business unit operations and employees access it
- Important to the mission of the organization
- Customers access data or are serviced by it
- Critical for incident response: need to determine criticality of incident, to identify patterns and problems, notification, and effective response
- Cybersecurity must know data to establish controls for data protection and security controls and to detect leakage
- Knowledge of data is important for business continuity, backup/recovery, and maintenance

Data Inventories: Minimum You Need to Know

- Data Description
- Data Type (PII, privileged, confidential, proprietary/IP, trade secret, public)
- Data Classification (H, M, L)
- Risk or Security Categorization (1-5)
- Data Format
- Data Owner
- Data Steward
- Data Custodian (controller, processor)
- Location of Data
- Data Protection Officer
- Security Officer
- Users
- Applications that use data

Digital Asset Management



Application Inventory

Data Inventory

Data Mapping

Information Security Controls

Usefulness During Coronavirus

- Know the users of sensitive data
    - Allow to work from home? Need owner approval? Access + download?
    - Extra controls needed? (Access controls, encryption, segmentation of data, policies and procedures) Extra monitoring or log analysis?
- Incident Response – prioritized, changes to procedures, special notifications
- Backup & Recovery – changes to current procedures? Extra coordination?
- Compliance & Notification
    - Operational changes that would impact privacy notices and terms of use for data?
    - Changes in notifications between controller and processor or users?
- Monitoring access and usage of data
    - Insider threat, detection of anomalies
    - Increased risk of disclosure to unauthorized party
    - Attacks may be harder to detect if coming from personal device