Data Governance for Risk Reduction and Value Creation

Neil Correa
Cyber Strategist, CIPP/C, CIAPP-P, CHFI
Security professionals must secure at the speed of Digital Business

- Embrace Big Data
- Protect Privacy
- Leverage Analytics & Machine Learning
- Open New Markets & Customers
- Support Hybrid IT/Cloud
- Increase Time to Value
- Secure DevOps
- Accessible Anytime Anywhere
The world is feeling the economic pressures

Rising cyber dependency due to increasing digital interconnection of people, things and organizations

2015
Attack on Ukraine’s power grid shut down 30 substations, interrupting power to 230,000 people

2016
SWIFT attack led to the theft of US$81 million from the central bank of Bangladesh

Today
Yahoo/Verizon and Starwood/Marriott M&A impact

Global interconnections continue to increase the attack surface

A Patchwork of Privacy Legislation Awaits...

PIPEDA (Canada)
CCPA (California)
LGPD (Brazil)
GDPR (EU)
POPI (South Africa)
FSS (Russia)
PIPA (South Korea)
APPI (JAPAN)
PDPB (India)
CDPR (China)
APA (Australia)

...without a single framework for compliance
Organizations needs a complete and reliable approach to navigate through the new world of privacy, risk and compliance.
Single Framework for Data Protection

- **Identify Sources**
  - Data for Disposition
  - Data Not In Scope

- **Classify**
  - In-Scope Data
  - Data for Disposition

- **Apply Policy**
  - Manage
  - Monitor
  - Notify
  - Move
  - Redact
  - Encrypt
  - Delete

- **Other**
  - Focus on only in-scope information
  - Apply analytics to high-value, sensitive information
  - Manage user rights to data use and enforce identity privileges
  - Build customer trust and confidence with controls
  - Protect data in use, in transit, and at rest--globally
  - Monitor for abnormal behavior and data exfiltration
Global Framework Addressing Data Privacy and Governance

**Identify**
- Personal data assessment

**Secure**
- Breach prevention

**Act**
- Encryption
- Breach Detection, Response & Reporting

**Analyze**
- Defensible Disposition
- Backup & Recovery

**Govern**
- Policy-Based Governance
- Litigation Management

- GDPR (EU)
- CCPA (California)
- LGPD (Brazil)
- CDPR (China)
- KVKK (Turkey)
- POPI (South Africa)
- PIPA (South Korea)
- PDPB (India)
- APPI (Japan)
- PIPEDA (Canada)
- FSS (Russia)
- APP (Australia)
- GDPR (EU)
Identify ➔ Personal Data Assessment

What and where is the information that will fall under these regulations?

Overview:
Determine data in scope of privacy regulations, and apply policies to move, redact, encrypt and dispose of personal data in accordance with privacy policy.

Benefits:
- Understand your privacy readiness and risk exposure
- Identify information that may be relevant to privacy requirements in an streamlined/automated fashion vs. a manual, error-prone process
- Systematically apply policies to applicable information for security, data protection, and lifecycle management purposes
- Protect against security breaches by proactively analyzing previously dark data that is more prone to breach
- Quickly automate and cost effectively ensure compliance-responsive data is encrypted
Analyze ➔ Defensible Disposition

How do I identify information for disposition, in accordance with erasure rights?

Overview:
Automatically identify structured and unstructured data for disposition that may be subject to privacy rights to erasure requirements, leading to lower storage costs and lower risk.

Benefits:
- Lower total storage costs by defensibly disposing of information (with audit trail) that costs € 23/GB to manage through its lifecycle (per ESG report).
- Ensure alignment with “right to be forgotten” and dispose of information that is no longer needed.
- Lower risk of information accidentally being viewed out of context.
- Protect against security breaches by proactively analyzing previously dark data that is more prone to breach.
Govern → Policy-Based Governance

How do I best apply and enforce policies to manage information through its lifecycle?

Overview:
Effectively apply and enforce data and identity-based policies to manage information privacy and access, while streamlining & driving cost efficiencies

Benefits:
- Understand your privacy readiness and risk exposure
- Identify information that may be relevant to privacy requirements in a streamlined/automated fashion vs. a manual, error-prone process
- Systematically apply policies to applicable information for security, data protection, and lifecycle management purposes
- Protect against breaches by proactively analyzing previously dark data, more prone to breach
- Manage information throughout its lifecycle in a consolidated repository that is protected and backed up in conjunction with privacy requirements to protect against fines & sanctions
How can I grow business while ensuring data is protected?

Overview:

Provide a proven, standards-based approach that meets criteria for use of data masking to protect personal data, without breaking business process.

Benefits:

- Proven, standards-based encryption and key management to protect sensitive data
- Meets GDPR guidelines for anonymisation and pseudonymisation—Format Preserving Hash (FPH) and Encryption (FPE) approach
- Supports collaboration inside and outside the organization
- Addresses the entire information lifecycle, including backup and recovery for a holistic approach, unlike other vendors with point solutions
Secure ➔ Breach Prevention

How can I neutralize the impact of a data breach?

Overview:
Find threats real-time, prevent data loss at field level, prevent unauthorized access and automatically identify application vulnerabilities

Benefits:
- If sensitive data is protected using encryption, breach notification is not required
- Adopt proven, standards-based encryption and key management technologies for protection of sensitive data-at-rest, data-in-motion and data-in-use throughout the enterprise.
- Automatically identify application vulnerabilities in source code and recommend code-level changes to remediate
- Automatically protect running .net and java applications from known vulnerabilities
- Adopt proven, standards-based encryption and key management technologies for protection of sensitive data-at-rest, data-in-motion and data-in-use throughout the enterprise.
# Data-centric Security is Critical for Privacy Control

## What is data-centric security?

**Data-centric**: Controls persist with the data itself, wherever it travels

- Unlike storage, network transport, systems, perimeter, etc. which act as a single control point

**Cryptography**: Encryption and tokenization (substituted values)

- Along with related key management processes to authorize data transformation

## What techniques apply for privacy use cases?

**Anonymization**: fully-obfuscated data, no longer “personal” after transforming

- “Johnny” → “Ypwkle” (Non-reversible) ...we use format-preserving hash (FPH)

**Pseudonymization**: reversible; replaces data with secure substitute value

- “Johnny” → “Ypwkle” (Reversible with key) ...we use format-preserving encryption (FPE)
Reliable Privacy is Your Catalyst to Value Creation!

Safe use of data for business analytic insights can help your organization **drive the top line**:

- Bring new products and services to market while preserving customer confidentiality from insights
- Identify new under-invested areas and optimize infrastructure while protecting intellectual property
- Learn more about buyer behavior, without compromising user loyalty or your reputation
- Drive greater productivity by managing your most sensitive data more responsibly, reducing waste

... and attain greater competitive advantage!
Data Governance Success Story: Regional European Telco

Compliance with national data privacy law and GDPR

- Subject to country-specific national privacy law and GDPR.
- Lack of visibility as to the volume, format and nature of personal data.
- Under major cost-saving pressure, looking for ROI.

Solution

- ControlPoint and Structured Data Manager for analysis, classification and elimination of ROT data.
- Content Manager enforced policy across 100 million records.
- Accessibility with data protection via Voltage SecureData encryption.

Result

- Established an privacy governance framework covering national privacy law and GDPR.
- Achieved storage cost savings by efficient records management, archiving and back-up.
- Achieved compliance risk reduction as Data Controller and Processor.
Security, Risk and Governance Solutions

IDENTITY & ACCESS MANAGEMENT
APPLICATION SECURITY
DATA GOVERNANCE & PROTECTION
ANALYTICS & MACHINE LEARNING
ENDPOINT SECURITY
SECURITY OPERATIONS
INFORMATION ARCHIVING