Cybersecurity Threats to Information Governance

PRESENTED BY:

JAMAL HARTENSTEIN, JD, CGEIT, CISSP, PMP, ITIL, MCP, SECURITY+

ARMA RECORDS KNOWLEDGE CONFERENCE – MAY 23. 2019

Presentation Agenda

- ✓ APPROACH
- ✓ TOOLS
- ✓ CHALLENGES
- ✓ GOVERNANCE

KAI PARTNERS

Approach

✓ Identify the following:
   1. What data you have.
   2. Who and what has access to it.
   3. Where it goes.
✓ Determine compliance exposure-based results.
✓ Regulations, standards, frameworks.
✓ Identify risk exposure.

Determine Compliance Exposure

Negligence Factors
- ✓ Duty
- ✓ Standard of Care
- ✓ Breach
- ✓ Causation
- ✓ Foreseeability (proximate cause)
- ✓ Damages

Assess Against Cybersecurity Frameworks

- ✓ National Institute of Standards and Technology (NIST)

- ✓ Center for Internet Security, Critical Security Controls (CIS CSC)

- ✓ Service Organization Controls (SOC)

- ✓ Payment Card Industry, Data Security Standard (PCI-DSS)

- ✓ International Organization for Standardization (ISO 27001)

- ✓ Cloud Security Alliance (CSA)

Information Governance Challenges

- ✓ Social Media and business transformation.

- ✓ Rapid expansion in laws and compliance regulation.

- ✓ Data Base Encryption, impact on enterprise strategy

- ✓ On-Premises versus Cloud solutions

Information Governance Challenges, cont.

✓Reconciling conflicting requirements between:
  ➢ Safety and reliability
  ➢ Privacy
  ➢ Cybersecurity
  ➢ Retention, disposition, and holds (Gov Code sec. 34090)

✓Disparate Information and 3rd Party Risk Management (TPRM)

✓Content producers

✓Federated services

✓Data Processors versus Data Controllers

KAI PARTNERS

Information Governance

- ✓ Security - prevention & Incident Response Planning (IRP)
- ✓ Regulatory compliance
- ✓ Business Intelligence(BI)
- ✓ E-Discovery and retention holds
- ✓ AB 2658 , Blockchain bill
- ✓ Integrity of information (CIA triad)
- ✓ Alignment hierarchy
- ✓ Reduce costs, reduce risk, increase value
- ✓ Monetizing in the Internet of Value

Governing – Blockchain & Smart Contracts

✓ Costs and consensus algorithms

✓ Private v. public

✓ IBM, AWS, Ethereum, Hyperledger, and Cardano with Haskell code language

Continuously Monitoring Protections and Defenses

✓ How are admins and security professionals securely managed?
   1. Privileged Access Management (PAM)
   2. Multi-factor Authentication
✓ Tools, software, solutions, protective measures
   1. Tokens
   2. Segmentation
   3. Least privileges & Need to know
   4. Mandatory vacation
   5. Security Information and Event Management (SEIM)
   6. Encryption w/ key management
✓ IRP management plan

Questions?