Tackling Risk Gaps in the Compliance Era

Tim Freestone, CMO
The confluence we are now in...

**I.T.**

- Mainframe Era
- Personal Computing Era
- Client/Server Era
- Enterprise Computing Era
- Cloud Era

**Cybersecurity**

- Mainframe Protection Era
- ARPANET Era
- Internet Protocols Era
- Viruses Era
- Hacker Era
- APT Era
Data Protection and Privacy Legislation Worldwide

- 71% COUNTRIES WITH LEGISLATION
- 9% COUNTRIES WITH DRAFT LEGISLATION
- 15% COUNTRIES WITH NO LEGISLATION
- 5% COUNTRIES WITH NO DATA

* According to the United Nations Conference on Trade and Development
## State Laws Signed To-Date

<table>
<thead>
<tr>
<th>State</th>
<th>Code</th>
<th>Law Title</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>California</td>
<td>CCPA</td>
<td>California Consumer Privacy Act</td>
<td>(2018; effective Jan. 1, 2020)</td>
</tr>
<tr>
<td></td>
<td>Proposition 24</td>
<td>California Privacy Rights Act</td>
<td>(2020; fully operative Jan. 1, 2023)</td>
</tr>
<tr>
<td>Colorado</td>
<td>SB 190</td>
<td>Colorado Privacy Act</td>
<td>(2021; effective July 1, 2023)</td>
</tr>
<tr>
<td>Connecticut</td>
<td>SB 6</td>
<td>Connecticut Data Privacy Act</td>
<td>(2022; effective July 1, 2023)</td>
</tr>
<tr>
<td>Virginia</td>
<td>SB 1392</td>
<td>Virginia Consumer Data Protection Act</td>
<td>(2021; effective Jan. 1, 2023)</td>
</tr>
<tr>
<td>Utah</td>
<td>SB 227</td>
<td>Utah Consumer Privacy Act</td>
<td>(2022; effective Dec. 31, 2023)</td>
</tr>
</tbody>
</table>

*According to the IAPP*
# Active Bills

<table>
<thead>
<tr>
<th>State</th>
<th>Bill(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hawaii</td>
<td>SB 974, SB 1110</td>
<td>Consumer Data Protection Act</td>
</tr>
<tr>
<td></td>
<td>HB 1497</td>
<td>(C)</td>
</tr>
<tr>
<td>Illinois</td>
<td>HB 3365</td>
<td>Illinois Data Privacy and Protection Act</td>
</tr>
<tr>
<td></td>
<td>SP 262, HB 346</td>
<td>(C)</td>
</tr>
<tr>
<td>Indiana</td>
<td>SB 0005, HB 1554</td>
<td>Kentucky Consumer Protection Data Act</td>
</tr>
<tr>
<td>Kentucky</td>
<td>SB 15</td>
<td>(C)</td>
</tr>
<tr>
<td>Maryland</td>
<td>HB 301, SB 698, HB 807</td>
<td>Online and Biometric Data Privacy Act (C)</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>HD 2281, SD 745, HD 3263</td>
<td>Massachusetts Data Privacy Protection Act (C)</td>
</tr>
<tr>
<td></td>
<td>SD 1971</td>
<td>Massachusetts Information Privacy and Security Act (C)</td>
</tr>
<tr>
<td></td>
<td>HD 2281, SD 255</td>
<td>Electronic Bill of Rights</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>SB 37/14, A 505</td>
<td>New Jersey Disclosure and Accountability Transparency Act (C)</td>
</tr>
<tr>
<td>New Jersey</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New York</td>
<td>SR 3162, A 4374, A 3593</td>
<td>Digital Fairness Act (C)</td>
</tr>
<tr>
<td></td>
<td>SB 365, HB 5277</td>
<td>New York Privacy Act</td>
</tr>
<tr>
<td></td>
<td>A 2587</td>
<td>New York Data Protection Act</td>
</tr>
<tr>
<td></td>
<td>SB 5655</td>
<td>It’s Your Data Act</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>HB 1030</td>
<td>Oklahoma Computer Data Privacy Act</td>
</tr>
<tr>
<td>Oregon</td>
<td>SB 619</td>
<td></td>
</tr>
<tr>
<td>Rhode Island</td>
<td>HB 5745</td>
<td>Rhode Island Personal Data and Online Privacy Protection Act</td>
</tr>
<tr>
<td>Tennessee</td>
<td>SB 73, HB 1138</td>
<td>Tennessee Information Protection Act (C)</td>
</tr>
<tr>
<td>Texas</td>
<td>HB 4</td>
<td>Texas Data Privacy and Security Act</td>
</tr>
<tr>
<td>Vermont</td>
<td>HB 121</td>
<td></td>
</tr>
<tr>
<td>Washington</td>
<td>HB 1616, SB 5640, SB 1337</td>
<td>People’s Privacy Act (C)</td>
</tr>
<tr>
<td>Minnesota</td>
<td>SB 950, HB 1892</td>
<td></td>
</tr>
<tr>
<td>Montana</td>
<td>SB 384</td>
<td>Consumer Data Privacy Act</td>
</tr>
</tbody>
</table>

*According to the IAPP*
Factors Determining Security Spending

- Best practices: 49%
- Compliance/regulations or mandates: 49%
- Evolving risks posed by changing workforce or business dynamics (e.g., hybrid/remote workforce): 41%
- Addressing risks that result from digital transformation (move to the cloud, etc.): 38%
- Responding to a security incident that happened in your organization (e.g., a breach): 35%
- Responding to a security incident that happened in another organization (news-cycle driven): 25%
- Mandates from the Board of Directors: 22%
- Responding to a security incident that happened in a business partner organization: 20%
- Partner mandates: 19%

Q: Which of the following factors help determine the priority of your security spending?
Data is at the center of Compliance…

- **Structured Data**
  (Databases)

- **Semi-structured Data**
  (Logs and Emails)

- **Unstructured Data**
  (Files and Email Data)

- **PII**

- **PHI**

- **IP**
Compliance Requirements

Structured Data
(Databases)

Semi-structured Data
(Logs and Emails)

Unstructured Data
(Files and Email Data)
The Growing Challenge – Data on the Move

- **Structured Data** (Databases)
- **Semi-structured Data** (Logs and Emails)
- **Unstructured Data** (Files and Email Data)

**PII**

**PHI**

**IP**
The Growing Challenge – Data on the Move

Structured Data
(Databases)

Semi-structured Data
(Logs and Emails)

Unstructured Data
(Files and Email Data)

CONTENT

PII

PHI

IP
Data Protection and Compliance Nightmare

Structured Data (Databases)

Semi-structured Data (Logs and Emails)

Unstructured Data (Files and Email Data)

CONTENT

PII

PHI

MOVING (Communicated)

Third Parties

Kiteworks 2023. All rights reserved.
Objective: Assess organizational maturity related to digital communications of confidential data

Surveyed over 780 IT, security, risk, and compliance professionals in 15 different countries

Targeted private sector enterprises in different industries such as manufacturing, finance, pharmaceuticals, healthcare, government, legal, and more

Asked them 45 questions about sensitive content communications privacy and compliance
Top Report Takeaways

PROBLEM: Organizations struggle to protect and control sensitive, unstructured data using traditional edge computing security and compliance protocols.

Nearly 75% of organizations indicate their measurement and management of sensitive content communications needs improvement.

62% of organizations experienced financial damage as a result of an attack on sensitive content communications.
According to Gartner

Data-Centric Security Will Be Key to a “Data Everywhere” World
According to Kiteworks

Data-Centric Security Will Be Key to a “Data Everywhere” World
Gap #1

Third Party Risk Management
Tackling the Issue: TPRM
Dynamic Risk Governance

The risk landscape has been changed by several important drivers, among them are:

- The increased interconnectivity of risks. As organizations have become more complex, risks have become more interconnected. Today's top organizational risks, such as supply chain, cybersecurity and third-party risk, all cut across large parts of the organization.

- The increased digitalization of organizations. This has meant the creation of new, fully digital risks, such as ransomware, as well as an increase in the speed and volatility of other risks such as third-party risk. Risks now change in their nature more often and quickly.

Hype Cycle for Cyber Risk Management, 2023
2022 Data Breach Investigations Report

Gain vital cyber security insights from our analysis of over 23,000 incidents and 5,200 confirmed breaches from around the world—to help minimize risk and keep your business safe.

Figure 36. Top Action vectors in System Intrusion incidents (n=3,403)
Triage Approach to Assessing Risks According to Gartner

1. Does the vendor access data? (Data sensitivity and volume)
2. Does the vendor access systems? (Criticality of the system)
3. Does the vendor support business processes? (Criticality of the process)

Assess vendor controls
Assess vendor security/risk capabilities
Assess vendor BCM/DR, incident response
Use focused questionnaires (e.g., SIG, SIFMA, etc.)
Validate controls

GAP

Analyze findings
Quantify risk impacts
Determine mitigation requirements
Determine contract implications

No or minimal assessment

And????
Manage cyber risk to mitigate financial risk.

NIST CSF

1st Party Ecosystem

3rd Party Ecosystem

XDR
SOAR
SIEM
EDR

MTD
MFA
EPP

DLP
CASB

SWG
EFW

IGA
CIEM

ZTNA

ITAM

GRC
ITVRM
S(C)RM
TPRM
(IT)VRM
### Close The Gap

1. Does the vendor access data? (Data sensitivity and volume)
2. Does the vendor access systems? (Criticality of the system)
3. Does the vendor support business processes? (Criticality of the process)

**Yes**
- Assess vendor controls
- Assess vendor security/risk capabilities
- Assess vendor BCM/DR, incident response
- Use focused questionnaires (e.g., SIG, SIFMA, etc.)
- Validate controls

**No**
- No or minimal assessment

**GAP**
- Protect interchange with encryption and DRM
- Control sharing with zero-trust principles at the content layer
- Unify content communication channels
- Track it all

**Analyze findings**
- Quantify risk impacts
- Determine mitigation requirements
- Determine contract implications
Gap #2
Zero Trust
Zero Trust

Zero Trust

- Identity Service
- Endpoints Accessing Apps
- The Network
- Applications (Cloud, On-Premises, SaaS)
Zero-Trust strategies tend to focus on technology access. Applications and workloads.

But what about the content that moves *through* and *beyond* applications and workloads?
To Put It Another Way

What Are Practical Projects for Implementing Zero Trust?

**Zero Trust (Security)**
- Security Mindset or Paradigm

**Zero Trust Strategy**
- Systematic Approach
- Replacing Implicit Trust With Adaptive Trust

**Zero Trust Initiatives**
- Specific Projects/Architectures
  1. User to Application Segmentation (ZTNA)
  2. Workload to Workload Segmentation (Identity-Based Segmentation)
  3. User-to-content segmentation
Data-centric Compliance Via Zero Trust Has Two Critical Layers

Applications & Workloads Layer

Content Layer [GAP]

Content doesn’t stay in the managed applications and workloads.
Gap #3

Digital Rights Management
Digital Rights Management

What is it?

What It’s Not
Digital Rights Management

According to Gartner....

Enterprise digital rights management offers persistent data-centric defense, solving security and compliance challenges with clear goals and governance. Security and risk management technical professionals should follow this EDRM framework when building use cases to design, implement and operate.
Digital Rights Management

A cryptographic element: Information is encrypted so that protection travels with data no matter where it moves or rests.

An identity element: Users must be authenticated and match policies related to specific user roles and groups before accessing rights-protected data on any system.

A granular usage control element: Users are granted specific rights within applications (such as the ability to only view, edit, print, copy/paste, or screen capture sensitive information).
Digital Rights Management

Administrator-defined protection of intellectual property (IP):

User-initiated protection of arbitrary files

Compliance-driven protection of regulated information
Today’s Approach to DRM is Legacy

“A cryptographic element: Information is encrypted so that protection travels with data no matter where it moves or rests”

Accomplished primarily as agent-based digital

- Issues in scale and functionality – low adoption
- File leaves the/a network – increased risk
Solutioning the Gaps
DISPARATE SYSTEMS  POOR TRACKING  NO CONTROL  WEAK SECURITY
A Private Content Network

A Kiteworks-enabled Private Content Network (PCN) unifies, tracks, controls, and secures the communication of private information.
**UNIFY**
Communication Channels

**TRACK**
Normalized audit trail to feed into SIEM or SOAR

**SECURE**
Movement of Content
- PII
- PHI
- PCI
- IP

**CONTROL**
Policy-driven rights management aligned to NIST CSF

**ONBOARD**
External Users and Systems
- Suppliers
- Accountants
- Employees
- Investors
- Partners
- Legal Counsel

**SYSTENS OF RECORD**
- Health Records
- Legal Documents
- Statements
- Employment Agreements
- Contracts
- Web Forms
- APIs
- File Sharing
- MFT

**PRIVATE CONTENT**
- Email
- Office 365
- G Suite
- Box
- Sharepoint
- Oracle

**LEGAL DOCUMENTS**
- Legal
- Employment Agreements
- Contracts

**PRIVATE CONTENT**
- Health Records
- Legal Documents
- Statements
- Employment Agreements
- Contracts
- Web Forms
- APIs
- File Sharing
- MFT
Enter Next-Gen DRM

Kiteworks SafeEDIT - sensitive data never even leaves your repository but can still be edited. No agents, no IRM, limitless scale and usability.
Just When You Thought It Was Safe to Go Back in the Pool

Enter: Artificial Intelligence Risk
The Exploding Problem

Generative AI a Top Emerging Risk for Organizations: Gartner Survey

Intellectual property, data privacy and cybersecurity are three areas that need to be addressed quickly, according to Gartner.

Don’t expect quick fixes in ‘re-teaming’ of AI models. Security was an afterthought.

Sensitive Biz Data to ChatGPT, Raising Security Fears

More than 4% of employees have put sensitive corporate data into the large language model, raising concerns that its popularity may result in massive leaks of proprietary information.
What is happening?

- Corporate Content
- Sensitive Data
- Employees & Third Parties
- Sensitive Data Leaking

- Training Data
- Knowledge Base
- Chat Interface
Why is the problem growing exponentially?

Because AI LLMs are exploding in offerings and use.
Further compounding the problem...

AI can be a BAD BAD Boy

Meet WormGPT, ChatGPT Alternative Without Boundaries, Ethics and Limits Used by Hackers

Meet PoisonGPT: An AI Method To Introduce A Malicious Model Into An Otherwise-Trusted LLM Supply Chain

New AI Tool 'FraudGPT' Emerges, Tailored for Sophisticated Attacks
Why is this happening?

SIMPLE:

Lack of content-based risk policies to prevent AI ingestion.
Solutioning: Content-defined Zero-Trust Controls w/ a PCN

Least privilege access policies defined at the content layer for Risk Reduction

Apply access and use controls by employees and third parties for “least privilege” access to content assets, defined by sensitivity of content assets.

Watermarking can be applied to alert users that specific content should not be used in AI LLMs.
Solutioning: Content-defined Zero-Trust Controls w/ a PCN

Content-defined ZT reduces risk, but even “allowed” users could technically still ingest sensitive content into LLMs.
Solutioning: View-only DRM protection with a PCN

Applying a Kiteworks view only policy to higher risk data, sensitive content cannot be downloaded and ingested into AI LLMs.
**Solutioning:** Next-gen DRM protection with a PCN

Applying Kiteworks **SafeEdit** policy ensures business productivity via collaboration can still be maintained without data leaving your network data center and repository, as only an editable video image streamed is transmitted.

*Available now in customers on KiteworksLABS and in first half 2024 for general access.*
Protect your sensitive content from AI Leaks

**High Risk**
Collaboration Required

**Moderate Risk**
Block Download

**Low Risk**
Control Access and Warn User

---

**Next-Gen DRM** – with SafeEDIT*
video streamed editing to block downloads and copy paste.

**View-only DRM** – Block downloads while still transmitting information.

**Content-defined Zero Trust Controls** – Least-privilege access and applying watermarks.

*Available now in customers on KiteworksLABS axnd in first half 2024 for general access.
To recap:

1) We’re in the compliance era together
2) Data is everywhere and so to should compliance controls, tracking and reporting
3) Some issues need to be tackled:
   - Zero-trust gap
   - TPRM gap
   - Antiquated approach to DRM
4) Data and privacy protection and compliance has a new vector to be addressed: AI
THANK YOU