Welcome To The 10th Annual Hacking Conference
Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!
Financial Services Hot Topic
Protecting Content on the Cloud

Bob Ertl
Sr. Director, Product, Kiteworks
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

COMPLIANCE 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 Data Privacy Regulations Signed To-Date

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

* According to the IAPP
...And More are on Their Way

* 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?
Agenda

1. The Compliance Era
2. Cloud Content Communication Risks
3. Impact of Cloud Cybersecurity and Privacy Risks
4. Risk Mitigation
5. Passing Audits With Reporting and Logging
6. How CMMC Affects Financial Services
7. Bonus: Protecting Sensitive Content From AI
Security & Compliance Risks of Sharing Content
Data is at the center of Compliance…

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

- Personally Identifiable Information
- Financial Information
- Intellectual Property
Compliance Requirements

Structured Data
(Databases)

Unstructured Data
(Files and Email Data)

Personally Identifiable Information (PII)

Financial Information

Intellectual Property

PROTECT

TRACK

CONTROL
The Growing Challenge – Data on the Move

Structured Data  
(Databases)

Semi-structured Data  
(Logs and Emails)

Unstructured Data  
(Files and Email Data)

Personally Identifiable Information

Financial Information

Intellectual Property
The Growing Challenge – Data on the Move

Structured Data
(Databases)

Semi-structured Data
(Logs and Emails)

Unstructured Data
(Files and Email Data)

Personally Identifiable Information

Financial Information

Intellectual Property
Data Protection and Compliance Nightmare

CONTENT

- Structured Data (Databases)
- Semi-structured Data (Logs and Emails)
- Unstructured Data (Files and Email Data)
- Personally Identifiable Information (PII)
- Financial Information
- Intellectual Property (IP)

MOVING (Communicated)

Third Parties

- Loss of visibility and control
- Inconsistent security measures
- Regulatory complexity
- Supply chain risk
According to Gartner

**Data-Centric Security Will Be Key to a “Data Everywhere” World**
But in the Compliance Era…

Compliance

Data-Centric Security Will Be Key to a “Data Everywhere” World
DISPARATE SYSTEMS
POOR TRACKING
NO CONTROL
WEAK SECURITY
Intentional and Inadvertent Sharing of Confidential Data

43% of Incidents Are Misdelivery
- Unintended recipients
- Unknown recipients
- Shared without controls

23% of Incidents Are Publishing Errors
- Wrong recipients

REASONS FOR INTENTIONAL SHARING
- Financial: 89%
- Grudge: 13%
- Espionage: 5%
- Convenience: 3%
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 financial services, manufacturing, legal, pharmaceuticals, healthcare, government, 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.

Nearly **62%** of organizations experienced financial damage as a result of an attack on sensitive content communications.

[kiteworks.com/sensitive-content-communications-report](kiteworks.com/sensitive-content-communications-report)
Risk Mitigation
Unify, Track, Control, and Secure Third-party Communication

**UNIFY Communication Channels**
- Private Content
  - Contracts
  - Financial Records
  - Statements
  - PII
  - Legal Documents
  - Tax Records
  - MFT
  - Email
  - APIs
  - Web Forms

**Public Internet**
- Public Content
  - Systems of Record
    - Oracle
    - SharePoint
    - Office 365
    - Google Drive
  - Public Content
  - Email
  - MFT
  - File Sharing
  - Web Forms

**SECURE Movement of Content**
- PII
  - Employee
  - Legal
  - Investors
  - M&A
  - Auditors
  - Loan Syndication
  - Legal Counsel

- Financial
  - Financial Records
  - Auditors
  - Investors
  - M&A
  - Regulators

- PCI
  - Financial
  - Financial Records
  - Auditors
  - Investors
  - M&A
  - Regulators

- IP
  - Financial
  - Financial Records
  - Auditors
  - Investors
  - M&A
  - Regulators

**ONBOARD External Users and Systems**
- Employees
- Legal Counsel
- Financial
- Financial Records
- Auditors
- Investors
- M&A
- Regulators
- Loan Syndication
**TRACK**

Pass Audits and Support SecOps

**Tracking Enables Compliance Audits & SOC**
- Comprehensive audit log
- Centralized, normalized, real time
- User, admin, system activities
- Custom and ad hoc reporting
- Canned reports for regulations

**Security Information and Event Management (SIEM)**
- Aggregates logs from across the infrastructure and apps
- Correlates events
- Monitors for incidents
- Built-in analytics
- Major vendors: Splunk, IBM QRadar, LogRhythm, etc.
UNIFY
Communication Channels

Systems of Record

Private Content

Contracts
Statements
Financial Records
Legal Documents

Email
APIs
Web Forms

TRACK
Normalized audit trail to feed into SIEM or SOAR

SECURE
Movement of Content

PII
Financial
PCI
IP

CONTROL
Policy-driven rights management aligned to NIST CSF

ONBOARD
External Users and Systems

M&A
Auditors
Employees
Investors
Loan Syndication

Regulators
Legal Counsel

Employees
Legal Counsel

Kiteworks 2023. All rights reserved.
CONTROL
Policy-driven rights management aligned to NIST CSF

DRM Policies Prevent Unintended Access
• Least-privilege defaults
• Granular access controls
• DLP with blocking & audit
• View-only with watermark
• Copy and forward controls
• File/folder expiration
• AIP sensitivity label content policies

Authentication Validates Identity
• LDAP / MSAD / SCIM / native
• Credentials, certificate, SMS OTP
• MFA (RADIUS, native), OAuth
• SAML 2.0, Kerberos, PIV/CAC

Admin Policies Minimize Insider Risk
• Admin cannot access content
• Separation of duties
• Folder ownership management
• Data sovereignty
• Legal hold for eDiscovery
Mitigation #1

Third Party Risk Management
Managing risks of sharing sensitive content:
- Regular risk assessments
- Contractual obligations
- Continuous monitoring
- Incident management
- Education and awareness
- TPRM in your data-centric security and compliance strategy
2022 Data Breach Investigations Report

Gain vital cybersecurity 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. IDENTIFY RISKS
   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)

   No or minimal assessment

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

   Yes

3. ANALYZE
   - How to manage data after vendor approval?
   - Quantify risk impacts
   - Determine mitigation requirements
   - Determine contract implications

GAP
Manage cyber risk to mitigate financial risk.

1st Party Ecosystem

3rd Party Ecosystem

NIST CSF

Identify

Protect

Detect

Respond

Recover

XDR

SOAR

SIEM

EDR

MTD

MFA

EPP

WAAP

AM

PAM

MFA

DLP

CASP

SWG

EFW

IGA

CIEM

ZTNA

ITAM

GRC

ITVRM

S(C)RM

TPRM

(IT)VRM
Close The Gap

1. IDENTIFY RISKS
   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)

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

3. ANALYZE FINDINGS
   - Quantify risk impacts
   - Determine mitigation requirements
   - Determine contract implications

GAP

• Control: zero-trust principles at the content layer.
• Protect: encryption and DRM
• Unify content communication channels.
• Track it all.
Mitigation #2

Zero Trust
Assume Attackers Have Infiltrated Your Organization

Principles
1. Always authenticate
2. Least privilege access
3. Micro-segment networks
4. Continuously monitor and analyze
The Cloud Security Alliance (CSA) recently published its latest report, CISO Perspective and Progress in Deploying Zero Trust. The study is based on interviews with security and risk management professionals and C-level executives who provided insights into current and future zero trust deployment plans. It found that

- 80% of C-level executives cite zero trust as a priority for their organizations, and
- 94% are implementing zero-trust strategies.

Ericom’s Zero Trust Market Dynamics Survey found that

- 80% of organizations plan to implement zero-trust security in less than 12 months, and
- 83% agree that zero trust is strategically necessary for their ongoing business.

CISOs must remove trust from tech stacks and define their unique strategy to adopt the framework.
Loss of protection, tracking, and controls when sensitive content moves to third-parties.
Sensitive content is now fully tracked and controlled with zero-trust principles applied.
Mitigation #3

Digital Rights Management (DRM)
Digital Rights Management

What is it?

What It’s Not

napster
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.
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).
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 your environment – increased risk
Enter Next-Gen DRM

Sensitive data never even leaves your repository but can still be edited. No agents, no IRM, limitless scale and usability.

Editsable Video of Sensitive Data Streams to User

Employees & Third Parties

No Download
No Copy Paste

Corporate Content Repositories w Sensitive Data

Content-based Risk Policy Controls

Safe EDIT

No Download No Copy Paste

Sensitive data never even leaves your repository but can still be edited. No agents, no IRM, limitless scale and usability.
Mitigation #5

Privacy Protection from AI
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, Gaining 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 Repositories w/ Sensitive Data → Sensitive Data Moves → Employees & Third Parties → Sensitive Data Leaking → AI LLMs

- 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 data encryption and content-based risk policies to prevent AI ingestion.
Solutioning: Content-defined Zero-trust Controls

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

Content-based Risk Policy Controls

Corporate Content Repositories With Sensitive Data

Sensitive Data Moves

Employees & Third Parties

AI LLMs
- Training Data
- Knowledge Base
- Chat Interface

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

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

Next-gen DRM. Sensitive data never leaves your repository but can still be edited.

Enforcing content-based risk 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.
Protect Your Sensitive Content From AILeaks

- **High Risk**
  - Collaboration Required
  - Next-gen DRM – With safe video streamed editing that blocks downloads and copy/paste.

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

- **Low Risk**
  - Control Access and Warn User
  - Content-defined Zero-trust Controls – Least-privilege access and applying watermarks.
Mitigation #6

CMMC
Cybersecurity Maturity Model Certification
CMMC
Cybersecurity Maturity Model Certification

- **What:** Framework for cybersecurity practices across DoD supply chain
- **Standard for:** Cybersecurity practice implementation and compliance verification
- **Required for:** All DoD suppliers including subcontractors
- **Required before:** October 2025 it will be included in all DoD contracts
CMMC
Content Classes Protected

FCI – Federal Contract Information
Requires protection but is not critical to national security
Most common for financial services organizations

CUI – Controlled Unclassified Information
Requires safeguarding or dissemination controls per laws, regulations, and government policies
# CMMC 2.0: 3 Levels

## Level 1
**Foundational**
- **Applies to:** Contractors working with FCI only
- **Regulation:** 17 practices
- **Annual Self-Assessment:** Attestation from senior company official

## Level 2
**Advanced**
- **Applies to:** Contractors working with CUI
- **Regulation:** NIST 800-171 (110 practices)
- **Certification:** Conducted and reported every three years year by accredited C3PAO

## Level 3
**Expert**
- **Applies to:** Contractors working with CUI on DoD’s highest priority programs such as developing parts for a weapons system or C&C communications system
- **Regulation:** NIST 800-172 (110+ practices)
- **Assessments:** Triennial assessments by Defense Industrial Base Cybersecurity Assessment Center audit teams
To recap:

1. We’re in the compliance era together
2. Data is everywhere – and compliance controls, tracking, and reporting should be everywhere too
3. Some issues need to be tackled:
   a) Third Party Risk Management (TPRM) gap
   b) Zero-trust gap
   c) Antiquated approach to DRM
4. Data and privacy protection and compliance have two new vectors to be addressed: AI and CMMC
THANK YOU


kiteworks.com/sensitive-content-communications-report
Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!
Speaker: Bob Ertl, Sr. Director of Product Marketing, Kiteworks

Title: Financial Services Hot Topic - Protecting Content on the Cloud

Synopsis:
In a fast-paced digital world, businesses rely heavily on email and file sharing to communicate and collaborate internally and with external parties. However, with the rise of cyberattacks and data breaches, secure file sharing has become an increasingly critical issue for organizations.

Financial services organizations rely heavily on exchanging and storing vast quantities of sensitive documents, making secure file sharing a critical component of their cybersecurity strategy. By implementing certain file sharing practices, these institutions can mitigate risks associated with unauthorized access, content breaches, and potential disruptions to critical infrastructure. And by instituting comprehensive audit logging and reporting practices, they can reduce the risks of adversarial and potentially failed regulatory audits.

In this talk, Bob will explore how organizations, particularly the financial services industry, play an important role in protecting critical infrastructure, based on professional experience and lessons learned from how companies implement cybersecurity measures.

At the end of the campaign, you will learn (takeaways):
• What good compliance and reporting means in the financial services space,
• How CMMC applies to financial services, and
• Why not having unresolved issues coming out of your financial risk management is important.

Date: November 6, 2023