Abstract:

In an era of increasing digital threats and a cloud-centric workflow, the traditional approach to security is no longer sufficient.

This presentation explores the evolving cybersecurity landscape faced by media, publishing, and entertainment organizations. It highlights the critical distinction between **security** (a tool's resistance to hacking) and **privacy** (a service provider's access to data), arguing that many common platforms are secure but not private.

The talk outlines a proactive strategy focused on foundational security practices, including the use of password managers, multi-factor authentication, and end-to-end encrypted messaging. It emphasizes the need for clear internal policies to govern the use of secure versus less-secure tools.

The discussion also addresses advanced topics such as the security risks of AI tools and the strategic importance of using alternative platforms with strong privacy laws. The presentation concludes that a successful cybersecurity posture in 2025 requires not just the right technology but a collective commitment to security-first practices.

A CISO’s Guide to Navigating the Security and Privacy Tradeoff

Ghalib Kassam, EVP CIO & CISO
Los Angeles Times

October 14, 2025

Disclaimer:

The information, views, and opinions expressed in this presentation are solely those of the presenter, Ghalib Kassam, and do not necessarily represent the official policy or position of **The Los Angeles Times**, its parent company, affiliates, partners, or any other employees.

This content is provided for informational and discussion purposes only.

No Official Representation: Nothing in this presentation should be construed as an official statement or endorsement by The Los Angeles Times.

Accuracy: While care has been taken to ensure the accuracy of the information provided, no warranties are made as to its completeness or correctness.

Personal Views: Any reliance you place on the information is strictly at your own risk. The presenter is speaking only in a personal capacity.

Introduction

- Goals and Objectives
- Why this topic
- 2 Case Studies, 5 Polls
- Q&A

The Current Threat Landscape

- Average Ransomware Payment in 2024: **$2.73M**[1]
- Breaches Involving Human Error: **68%**[2]
- Median Discovery Time to Detect Breach: **51 Days**[3]
- US Average Cost of Data Breach: **$9.36M**[4]
- Cybercrime is projected to cost **$10.5T**[5] - globally in 2025.

⚠ **Critical Reality:** These breaches did not result from a lack of ***security***—many platforms are secure—but from a **lack of *privacy*** and **poor data governance**.

Sources:
1: Sophos (link)
2: Verizon 2024 DBIR (link)
3: Verizon 2025 DBIR (link)
4: Statista/IBM Global Report (link)
5: VikingCloud (link)

Security vs. Privacy: The Critical Distinction

While security focuses on safeguarding data from threats, privacy emphasizes controlling how personal information is accessed, used, and shared

🔒 **Security**:
Tool's resistance to hacking. Can a bad actor break in?

🛡️ **Privacy**:
Provider's access control. Can the provider see your data?

⚡ **The Gap**:
Many platforms **may be secure** but **NOT always private**. For example, **Google Drive is secure**, but **not private.** However, **Signal** is **both secure and private**, it is *end-to-end encrypted*,

Tip: Adopt a tiered approach—use **secure tools** for *public content*, and **private, encrypted tools** for *sensitive source communications*.

Poll #1: Access Review Frequency

How often does your organization review which employees have access to sensitive content?

OPTIONS:

1. Daily/Weekly
2. Monthly
3. Quarterly or Less
4. Never Formally

(Submit your response to the poll displayed on your screen)

Case Study: MGM & Caesars Vishing

What Happened: In 2023 attackers found MGM and Caesars employees on LinkedIn, impersonated them, and called the service desk requesting account access. Service desk granted access based on caller knowledge alone.

📞 **The Attack (Vishing)**: MGM detected suspicious activity and eventually shut down Okta and Azure infrastructure, but attackers retained super-administrator access and Global Administrator privileges in parallel systems.

Result: Ransomware deployed across 100+ ESXi hypervisors, 100+ Las Vegas properties crippled, Slot machines down, ATM systems down, Digital key cards inoperative, and Reservation systems offline. Staff reverted to pen and paper. **MGM took $100M hit** to Q3 earnings. Caesars **paid $15M ransom** instead of recovery.

Key Lesson: It took just one unauthenticated vishing call to bypass enterprise-grade security. Service desk must require "something you have" (MFA), not just "something you know" (knowledge-based questions attackers can research on most social media platforms such as LinkedIn).

The Foundational Pillars: Non-Negotiable Practices

The most effective and affordable security measures are **not complex** or **expensive**. They are the basics, and they are a powerful line of defense.

🔑 **Password Managers & Passkeys**
Eliminate password reuse. Deploy encrypted password managers like 1Password or Bitwarden across the organization.

✅ **Multi-Factor Authentication**
Enforce MFA on all critical systems, email, and VPN access. FIDO2 keys are most secure; authenticator apps second.

🔐 **Encrypted Messaging**
Use Signal or ProtonMail for sensitive communications. End-to-end encryption prevents provider access.

These three practices eliminate 80% of common attack vectors. They're not optional in 2025—they're the baseline.

Poll #2: Executive MFA Status

Is MFA currently mandatory for your senior executives' email?

OPTIONS:

1. Yes, organization-wide
2. Yes, but selective roles
3. In progress
4. Not yet

(Submit your response to the poll displayed on your screen)

Case Study: Samsung ChatGPT Incident[1]

🚨 **What Happened**: Samsung engineers pasted proprietary source code and hardware specifications into ChatGPT to optimize their work. Their **semiconductor IP**, **design documents**, and **technical specifications** now lives **permanently** in **OpenAI's training data**.

Immediate Response: Samsung discovered the leaks within 4 weeks, launched internal investigation, and found 65% of employees acknowledged GenAI security risks.

The Ban: On May 1, 2023, Samsung (**temp**) banned all generative AI tools (ChatGPT, Bing, Bard) across all company devices and networks.

Key Lesson: **Convenience overrides security** unless **policy comes first**. Even senior engineers at one of the world's most sophisticated tech companies will submit sensitive data to easy-to-use tools if there's no explicit policy prohibiting it. **Policy must precede technology enablement**.

Sources:
1: Cyber Security Hub (link)

Building Your **Policy Framework**

Principle: **Clear policies** must **govern which tools** are used for **which data classifications**.

❌ **No Policy Scenario**:
Employees default to convenient tools. Confidential IP end up in Slack, MS Teams, WhatsApp. IP shared via personal Gmail. One breach exposes everything.

✅ **Policy-Driven Scenario**:
- Public information → standard tools.
- Confidential content → encrypted, audited platforms only.
- Unclassified employees cannot access unreleased content.

Key Policies Needed (not exhaustive):
- Data Classification Matrix (Public/Internal/Confidential/Restricted)
- Tool Approval List (approved vs. prohibited tools by data type)
- Access Control Matrix (who accesses what, when, why)

The "AI" Slide: AI Tools have Security Risks

⚠ **Warning**: GenAI tools like ChatGPT are **NOT** private. **Your** data trains **their** model. Data Vacuum Cleaners

Key Statistics:

- **55%** of Global Employees Use Unapproved GenAI[1]
- **67%** Have Leaked Confidential Data[2]
- **$5M - $7M**: Potential Damage from IP Exposure[3]

Recommendation:

- Deploy enterprise* GenAI solutions (Microsoft Copilot Pro, Claude for enterprise).
- Make sure you have a **Data Processing Agreement** (DPA), **contractually guaranteeing** no data training, clarity of **data ownership**.
- **NOTE**: Make a Data Processing Agreement (DPA) central to every MSA, PSA, SoW contractual agreement whenever someone will be hosting your data!!

Sources:
1: Tanium (link)
2: Metomic.io (link)
3: IBM Report (link)

AI, Alternative Tools, and The Future

As we look ahead, we must also consider the security implications of emerging technologies.

- **AI Tools**: Many AI tools, particularly generative AI models, **send data to a third-party** service provider for processing. This creates a significant **security vulnerability**. If you're using an AI tool with **sensitive** or **proprietary** information, you're essentially "**blasting a hole** through your information security."
- **Jurisdiction**: The **physical location of a server matters**. Some companies choose to house their data **outside the United States** to protect against U.S. law enforcement requests. This, too, has tradeoffs and requires careful consideration of foreign legal risks, but it is a strategic option that we must be aware of.

Strategic Privacy: Choosing Vendors by Data Residency

Why Geography Matters:
Data stored in Switzerland, Iceland, or EU is **protected by stricter privacy la**ws than US-based servers. Server location determines which government can legally access your data.

🇨🇭 **Switzerland**:
Strong privacy laws, no mass surveillance, companies like ProtonMail operate here. Best for sensitive content.

🇪🇺 **European Union**:
GDPR compliance is mandatory. Stricter than US.

🇺🇸 **United States**:
Subject to subpoena requests. Acceptable for non-sensitive ops, but should be avoided for IP.

Poll #3: Biggest Security Challenge

What's your organization's biggest security challenge?

OPTIONS:

1. Employee security awareness
2. Legacy system vulnerabilities
3. Third-party vendor risk
4. Cloud/remote access security

(Submit your response to the poll displayed on your screen)

When an Incident Happens: Response Framework

🚨 **Immediate** (0-1 Hour):
Isolate affected systems. Notify the incident response team. Preserve evidence. **NOTE**: Do NOT pay ransom… unless

📋 **Short-term** (1-24 Hours):
Determine scope. **Notify** affected parties. Engage FBI/law enforcement. Brief leadership.

🔍 **Long-term** (Days-Weeks):
Full forensic analysis. Root cause determination. Remediation. **Communicate** transparently to stakeholders.

Critical:
Have a written Incident Response Plan **BEFORE** you need it. Test it **quarterly**. Leadership must understand their roles—especially around disclosure timelines and stakeholder communication. **Practice**, **Practice**, **Practice**

Poll #4: Incident Response Plan Status

Does your org have a documented, tested incident response plan?

OPTIONS:

1. Yes, tested within 6 months
2. Yes, but not recently tested
3. Partially documented
4. Not yet in place

(Submit your response to the poll displayed on your screen)

Your 90-Day Security Roadmap

Month 1: Foundation
- Deploy password managers/Passkeys
- Mandate MFA for everyone*
- Security awareness training, Phishing Campaigns

Month 2: Structure
- Data classification policy*
- Establish a Business Continuity Plan
- Vendor audit

Month 3: Resilience
- Incident response drill
- Data Backup verification
- Data Restoration verification

Security is not a destination—it's a continuous practice. Assign clear ownership. Measure progress. Report regularly to the board*.

Poll #5: Primary Security Priority

What's your primary security priority for next 90 days?

OPTIONS:

1. Improve access controls
2. Enhanced monitoring/detection
3. Employee training & awareness
4. Vendor risk management

(Submit your response to the poll displayed on your screen)

Key Takeaways: The Security-First Mindset

1. Know the Difference: Secure ≠ Private. Evaluate both dimensions when selecting platforms.

2. Foundation First: Password managers, Passkeys, MFA, encrypted messaging stop 80% of attacks. Get these right before worrying about advanced threats.

3. Policies Drive Behavior: Clear data classification and tool usage policies are more effective than technology alone.

4. AI is Powerful but Risky: GenAI tools leak data. Deploy enterprise solutions with contractual data protections.

5. Geography Matters: Where data lives determines who can legally access it. Swiss/EU hosting for sensitive IP.

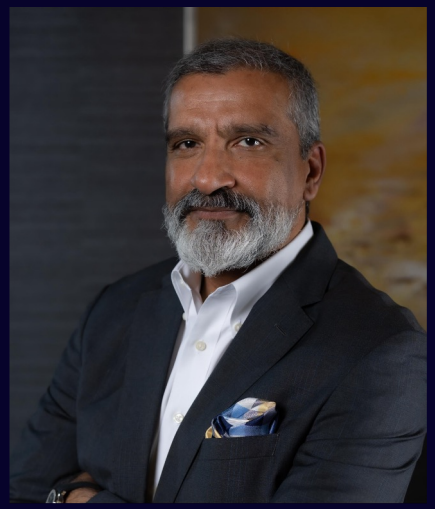
6. Be Ready: Incidents will happen. Have a tested response plan. Transparency and speed matter more than perfection.


Q&A / Thank You

Contact Info:

Ghalib Kassam is the Executive Vice President (EVP), Chief Information Officer (CIO), and Chief Information Security Officer (CISO) at the California Times (Los Angeles Times). He directs the complex cybersecurity, digital, data, and information technology transitions that underpin the news organization's core mission and drive its overall business transformation. With over 25 years of experience in global IT and management consulting, Ghalib is a seasoned leader known for his ability to align technology investment with measurable business outcomes and optimize operational service performance through continuous improvement initiatives. His international career spans high-stakes sectors, including media, healthcare, aerospace & defense, and insurance.

Ghalib is a highly engaged thought leader, contributing to industry discourse on navigating the complexities of the media sector and the evolving AI threat landscape, often speaking at forums like the Southern California CIO and CISO communities. He is a hands-on executive who leverages diverse teams to drive metric-based results. He holds an M.B.A. from the University of Phoenix and remains committed to community service, serving on the boards of FOCUS Humanitarian Assistance and High Tech Los Angeles, Innovate@UCLA, Gartner Southern California CIO & CISO Community, and ISACA-LA.



Ghalib Kassam

ghalibkassam@linkedin.com