

Kiteworks Survey Finds 80% of Organizations Hit by Security or AI Incidents Last Year

*AI Readiness Score of 16 Out of 100
Exposes a Critical Controls Gap*

SAN MATEO, CA, UNITED STATES, July 30, 2026 /EINPresswire.com/ --

Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, today released its [2026 Data Security and Compliance Risk: Annual Survey Report](#), based on primary research with security, compliance, risk, and IT professionals across 10 industries and three global regions. Now in its fifth year, the finding is stark. Eighty percent of organizations experienced at least one security or AI-related incident in the past 12 months, not a projected risk but a reported outcome.

“

Organizations have deployed AI far faster than they've built the governance infrastructure to manage it.”

*Tim Freestone, Chief Strategy
and Marketing Officer at
Kiteworks*

The incidents came with consequences. Sixty-three percent of organizations experienced a compliance outcome, such as an audit finding, a required remediation plan, a board escalation, a contractual penalty, or a formal regulatory investigation. And 65% discovered employees using unapproved AI tools with sensitive organizational data.

What sets this report apart is how the numbers are derived. Rather than self-reported confidence, it scores

organizations on deployed controls, what is technically operational. The Data Security Maturity Score (DSMS) evaluates 11 binary security controls, 8 general ones protecting everyday human-driven data access and 3 AI-specific. The AI Governance Maturity Score (AIGMS) measures 19 AI and agent governance capabilities. Neither can be inflated by perception. The results are stark. It found a mean DSMS of 39 out of 100, a mean AIGMS of 35 out of 100, and a combined Data Security and Compliance Readiness Index (DSCRI) of 16.2 out of 100. Seventy percent of organizations sit in Tier 1 or Tier 2, developing maturity at best. Read together, the two scores show whether controls are keeping pace with both people and agents.



“Organizations have deployed AI far faster than they’ve built the governance infrastructure to manage it,” said Tim Freestone, Chief Strategy Officer at Kiteworks. “The incidents have already happened, and the compliance consequences are already being felt. The path forward is architectural. It requires a data policy engine that enforces controls at the data layer for every person and every agent alike, not behavioral policy people can route around. Organizations that reached Tier 4 maturity got there by deploying controls, not documenting intent.”

The governance gap is measurable. No AI containment control in the survey is deployed by more than 31% of organizations. Fifty percent cannot produce a complete AI data access audit record within one business day, a direct exposure under DORA, NIS2, and the EU AI Act. Seventy-three percent have no technical enforcement over which channels employees can use for sensitive data, and only 27% have deployed AI-specific DLP.

The shadow AI problem is equally structural. Among organizations that discovered employees using unapproved AI tools, 36% found customer and client data flowing through them, 33% found IT credentials, and 31% found employee personal and HR data. The 35% reporting no discovery likely lack the detection capability to see it.

“AI risk is no longer a future problem. It is a present condition most organizations are still treating as a planning exercise,” said Patrick Spencer, SVP of Americas Marketing and Industry Research at Kiteworks. “Organizations still waiting to act are behind, not ahead. This research gives leaders defensible data grounded in deployed controls, not stated intentions, the foundation for moving investment toward architecture that governs people and agents under one standard.”

The gap between the top and bottom of this survey is 38 DSCRI points. The 19% of organizations in the Resilient quadrant (DSMS and AIGMS both at least 50) carry a mean DSCRI of 46. The 66% in the Exposed quadrant (both below 50) carry a mean DSCRI of 8, despite similar industry and



Big security budgets don't always translate to better security.



AI governance is "less bad" relative to other regions.

size mixes. The difference is deployed AI governance controls. At the survey mean DSMS of 39, raising AIGMS from 35 to 60 adds roughly 10 DSCRI points, nearly double the gain from adding four security controls while AIGMS stays fixed. The report identifies seven priorities for closing that gap:

- Classify and enforce sensitive data
- Deploy AI-specific DLP through a centralized policy engine
- Integrate MFT and AI infrastructure with a SIEM
- Implement and test an AI kill switch
- Build audit trails that meet regulatory production timelines
- Assign dedicated AI data governance ownership
- Consolidate sensitive data exchange platforms

The full report includes industry, regional, and organization-size breakdowns, and a Security Maturity Readiness Checklist for prioritizing remediation investment.

Download the 2026 Data Security and Compliance Risk: Annual Survey Report.

The research was conducted by Centiment on behalf of Kiteworks in Q2 2026.

About Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

David Schutzman

Kiteworks

+1 203-550-8551

david.schutzman@kiteworks.com

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[TikTok](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/930014838>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.