RISK COVERAGE HUB · WILLIAM TYGART OPINION

In 1893, Fire Underwriters Refused to Insure Unfused Wiring. Cyber Underwriters Are Hitting the Same Wall on AI OAuth.

By Will Tygart · Published November 27, 2026 · Two-Page Underwriting Reference

Direct Answer: Fire insurers solved rampant electrical blazes after the 1893 Chicago World's Fair by refusing to bind coverage without independent testing, founding Underwriters Laboratories in 1894 and unifying the National Electrical Code in 1897. Cyber underwriters face an identical OAuth wiring gap today, which brokers can mitigate immediately with CASA-verified apps and isolated Workspace airlock accounts.

1. Why Fire Insurers Built the Electrical Safety Code First

Before governments regulated household electricity, property underwriters hit an existential loss problem. At the 1893 Chicago World's Fair, over 100,000 incandescent bulbs and rushed wiring kept sparking construction fires. Fire syndicates hired 24-year-old engineer William Henry Merrill Jr. to inspect the grounds; in 1894 they backed his $350 testing room above Fire Patrol Station No. 1, creating Underwriters Laboratories, and by 1897 insurers and engineers published the first National Electrical Code (NFPA 70). Risk transfer only scaled once underwriters could verify a testing stamp and a breaker panel.

Fire Underwriting Era (1893–1897)	What Underwriters Faced	Cyber Underwriting Era (2026)	Verifiable OAuth Control
1893 Chicago World's Fair	100,000+ incandescent lamps and unvetted AC wiring sparked construction fires	Rapid SaaS and AI agent adoption across mid-market insureds	Inventory every third-party OAuth Client ID granted Workspace tokens
William Henry Merrill Jr. ($350 Lab, 1894)	Fire syndicates funded independent testing above Fire Patrol Station No. 1	Brokers cannot pentest 40 AI vendors on a $15,000 cyber account	Require App Defense Alliance CASA (OWASP ASVS) validation for restricted scopes
Edison Safety-Conductor (US227226)	Enclosed sacrificial lead wire melted safely inside an insulated tube	Primary admin/founder seats hold years of PII, banking, and password resets	Isolate third-party AI intake on a dedicated $7/mo Workspace airlock seat
1897 National Electrical Code (NFPA 70)	Replaced conflicting city rules with one standardized wiring code	Unconfigured SaaS portals leave 'Allow any OAuth app' enabled by default	Lock Admin API controls to Sign-in only and enforce drive.file / draft-only scopes

2. From Theoretical Compute Warranties to Today's OAuth Gate

- **Existing UL-Equivalent Vetting:** External AI tools requesting restricted Gmail or Drive scopes must clear App Defense Alliance CASA audits built on OWASP ASVS annually.
- **Shared Responsibility Still Applies:** Google secures transport, authenticates identity, and kills rogue OAuth Client IDs globally—but cannot stop an over-scoped token an insured voluntarily clicked 'Allow' on.
- **Immediate Renewal Action:** Pair Workspace Admin Console API lockouts with a $7/month sacrificial airlock account so third-party AI risk sits in a 30 GB blast zone instead of the CEO's mailbox.

3. Four Controls Brokers Should Verify Before Binding Cyber & Tech E&O

In an earlier Risk Coverage Hub analysis, we examined how theoretical cryptographic compute warranties would separate ledger bugs from stolen keys. You do not need to wait for theoretical hardware to underwrite AI connectivity today—every carrier can ask four concrete OAuth questions on the next renewal.

Supplemental App Question	Weak 'Yes' (Extension-Cord Risk)	Strong Underwriting Proof (Breaker Panel)	Statutory / Standards Anchor
Third-Party AI App Governance	Employees authorize any AI notetaker or assistant via click-through OAuth	Admin Console restricts unconfigured apps to basic Sign-in only; explicit allowlist	Google Workspace Admin API Controls
Vendor Security Validation	Vendor self-attests privacy on a marketing landing page	Vendor clears annual third-party CASA lab audit for Gmail/Drive scopes	App Defense Alliance CASA / OWASP ASVS
Token Blast-Radius Limit	AI tools hold broad read/write tokens on executive or finance mailboxes	AI interacts strictly with a $7/mo sacrificial seat holding 0 legacy archives	NIST SP 800-207 Zero Trust Containment
Service-Provider Oversight	No written inventory or periodic review of connected SaaS tokens	Quarterly OAuth token-grant audit log export tied to incident revocation plan	16 CFR Part 314.4(f) Safeguards Rule

4. Broker Pre-Submission Checklist

- **Audit** `Unconfigured third-party apps`**:** Confirm `admin.google.com` restricts unvetted tools to `Sign in with Google` basic info only.
- **Separate AI intake from crown-jewel seats:** Verify external AI agents connect exclusively to a dedicated `$7/mo` sacrificial Workspace seat.
- **Export OAuth token-grant logs:** Document quarterly review of connected Client IDs to satisfy `16 CFR 314.4(f)` service-provider oversight.
- **Verify vendor cancellation playbooks:** Confirm staff can revoke a compromised AI Client ID in under 60 seconds without halting billing or claims intake.

5. Primary Historical, Regulatory & Technical Sources

- UL Solutions — 1893 Chicago World's Fair & William Henry Merrill Jr. History
- NFPA — National Electrical Code (NFPA 70) Standards Access
- U.S. Patent 227,226 — Edison Safety-Conductor for Electric Lights (1880)
- App Defense Alliance — CASA Cloud Application Security Assessment
- OWASP — Application Security Verification Standard (ASVS)
- Google Cloud Help — OAuth App Verification & Annual Security Audits

Educational commentary for insurance and risk professionals only; not legal advice, coverage placement, or a binding policy endorsement.