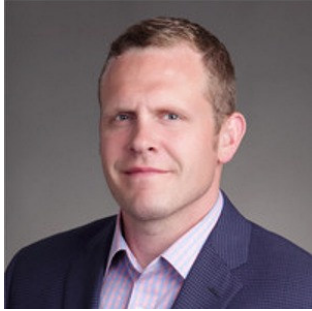




#21

Taylor Lehmann

Deputy CISO and Head of the Office of the CISO
Salesforce

Public role source revisited. Employer/self sources and association/event biographies are distinguished; direct role acceptance is not established. **Current-role source**

Direct business email and telephone: not publicly verified.

LinkedIn profile | Named professional biography / public route

Work base: Not established from reviewed sources. Actual work base, DC access and willingness require direct confirmation.

Recommendation and rationale

Reserve / second-group qualification. Company-employed deputy CISO and substantial governance work; validate enterprise scope and company benefit.

Research rank #21 - Sector qualification. Final research recommendation for this pass; ISA selection and outreach approval pending.

Company capacity and proposed benefit

FY2026 revenue \$41.5bn. Own announcement states Salesforce move in June 2026; earlier Google views are historical. **Source:** www.salesforce.com

Proposed company benefit: Validate which of those priorities are relevant to his new Salesforce remit.

Proposed executive benefit: Contribute his prior AI integrity and healthcare resilience experience.

What This Recruit Could Add to ISA

Create an AI provenance and critical-service continuity case with accountable release decisions. **Source:** www.healthcaredive.com

Handbook connection: Tool E 48-50; B 37-40. Proposed output and benefits require agreement. **Source:** www.nacdonline.org

Introduction and next decision

No named introducer established. ISA to designate an approved contact route; no private relationship inferred.

ISA to reconcile account status and route; then validate current remit, contribution, corporate payer and participation directly.

Policy history and board-selection fit

Policy / governance discussion: Public governance and disclosure commentary; distinguish analysis of rules from government policymaking.

No additional authoritative policy-history evidence was established in the deeper check. This is an evidence gap, not proof of no policy involvement.

Benchmark: ISA recommendations, current ISA board practitioner profile, operating authority, company capacity, attributable policy work, concrete contribution, and portfolio balance. Corporate directorship alone does not determine priority.

Qualification status and ownership

Requirement	Evidence and remaining confirmation
Current role	Public role support; recheck directly before contact; direct confirmation pending.
ISA membership	Unknown current company/account and designated-representative status. Public board absence does not establish nonmembership.
Eligibility	Operating practitioner fit supported by research. ISA acceptance and employer designation pending.
Board feedback / introducer	No named introducer established. Introduction completion: not confirmed.
Corporate sponsorship	Published annual dues \$75,000; corporate payer, budget approver and written authorization not confirmed.
Executive interest	Not directly confirmed. Published interest in cyber topics is not membership interest.
Time / participation	Four meetings yearly, including two in Washington, DC and two virtual, plus agreed preparation. Availability, travel and term commitment not confirmed.
ISA output and benefits	Person-specific hypotheses documented; prospect and employer acceptance not confirmed.
Portfolio	Industry/expertise rationale assessed. Work base and DC access require direct confirmation.

ISA public board / meeting baseline | Bylaws | Published sponsorship

1631 owns researched case and source accuracy; ISA owns current membership/eligibility/introducer decision; employer/prospect must confirm funding, interest, availability and proposed output.

Image and contact provenance

Portrait: Exact named source asset; manually selected. Source: www.rsaconference.com

Company mark: Exact named source asset; manually selected Source: www.salesforce.com

Attributable commentary and evidence ledger

10 / 10 substantive sightings recorded. Depth target met.

1. How the generative AI boom changes healthcare cybersecurity | Healthcare Dive

February 2026 | Direct interview [Source: www.healthcaredive.com](https://www.healthcaredive.com)

Discusses AI integrity and provenance, including model documentation and signing, because harmful output can be hard to distinguish from mistakes.

Attribution / limitation: Spoke while at Google Cloud; current Salesforce sponsorship and relevance need validation.

2. The real cost of healthcare cybersecurity breaches - Help Net Security

November 13, 2023 | Direct Q&A [Source: www.helpnetsecurity.com](https://www.helpnetsecurity.com)

Connects healthcare cyber breaches to patient harm and care delivery rather than treating them solely as data-loss events.

Attribution / limitation: Historical Google healthcare role; not a Salesforce policy statement.

3. Why CISO Taylor Lehmann couldn't pass up coming to Google

November 30, 2023 | Direct interview [Source: www.itbrew.com](https://www.itbrew.com)

Discusses security programs aligned with actual organizational risk and practical execution, rather than relying only on rules.

Attribution / limitation: Historical role; validate whether this remains a priority at Salesforce.

4. Cloud CISO Perspectives: How Google is helping to improve rural healthcare cybersecurity | Google Cloud Blog

2024 | Attributed Google company commentary [Source: cloud.google.com](https://cloud.google.com)

Describes efforts to support rural healthcare cybersecurity and protect service delivery in organizations with limited security resources.

Attribution / limitation: Company program context and historical affiliation; does not establish Salesforce support for that program.

5. Cloud CISO Perspectives: 2024 Cybersecurity Forecast - Lehmann contribution

December 21, 2023 | Named contribution in employer publication [Source: cloud.google.com](https://cloud.google.com)

Predicts that CISOs will seek legal support, insurance and explicit board/executive accountability after new disclosure requirements. Rejects treating cybersecurity outcomes as the CISO's responsibility alone.

Attribution / limitation: Only the paragraph labeled Taylor Lehmann is attributed to him. This is a historical forecast from his Google role, not current Salesforce policy or legal advice.

6. Health-ISAC gains Google Cloud as ambassador

July 21, 2022 | Direct SC Media interview [Source: www.scworld.com](https://www.scworld.com)

Describes a collaboration without special sales conditions: Google practitioners would join working groups and produce concrete outputs on shared healthcare problems. Argues that interdependent providers need community knowledge and support, particularly organizations with limited security resources.

Attribution / limitation: Only Lehmann's attributed comments are used. Historical Google/Health-ISAC role; does not establish Salesforce sponsorship interest or access to sensitive community data.

7. Cloud CISO Perspectives - healthcare continuity and shared defense

July 31, 2023 | Lehmann-authored guest column in Google publication [Source: cloud.google.com](https://cloud.google.com)

Relates healthcare cybersecurity to keeping essential care available. Advocates secure design, attention to medical-device dependencies and practical threat-sharing collaboration through Health-ISAC.

Attribution / limitation: Only the section explicitly by Taylor Lehmann is attributed to him. Historical Google role; cloud benefits are publisher claims, not an independent Salesforce assessment.

8. Hospital cybersecurity goals: availability and implementation constraints

February 5, 2024 | Direct interview with The Register [Source: www.theregister.com](https://www.theregister.com)

Warns that basic safeguards can be difficult to implement without disrupting care. Calls for resilience and recovery alongside prevention, with service availability treated as a central security objective.

Attribution / limitation: Historical Google interview. His prediction that voluntary goals would become mandatory is a dated forecast, not a verified current legal requirement. Other organizations' incidents are not his own experience.

9. mWISE 2024: measuring resilience and validating supplier safeguards

September 2024; exact recording day unverified | Guest interview; full theCUBE transcript [Source: www.thecube.net](https://www.thecube.net)

Calls for better risk quantification and communication. Recommends testing whether controls actually work, knowing dependencies and validating secure design rather than relying on supplier questionnaires alone.

Attribution / limitation: Guest responses are separated from interviewer prompts. Historical Google interview, not current Salesforce policy; no claim that a framework guarantees resilience.

10. How healthcare can strengthen its own cybersecurity resilience

February 11, 2022 | Coauthored Google article with Seth Rosenblatt [Source: cloud.google.com](https://cloud.google.com)

The coauthors recommend valuing assets by their role in patient care and business operations, threat modeling changes in technology and providers, and progressively demanding exercises involving clinical, legal, communications and supplier teams.

Attribution / limitation: Joint authorship; recommendations are not assigned solely to Lehmann. Historical healthcare/Google context; does not establish current Salesforce controls.