



#19

James Nettesheim

Chief Information Security Officer and Enterprise Technology
Lead

Block

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. Enterprise operating scope, joint advocacy and practical governance; no formal testimony established.

Research rank #19 - Priority qualification. Final research recommendation for this pass; ISA selection and outreach approval pending.

Company capacity and proposed benefit

FY2025 Form 10-K reports 10,205 full-time employees and approximately \$10.36bn gross profit. Gross profit is explicitly not revenue. **Source:** www.sec.gov

Proposed company benefit: Test Block's evidence for safe AI use and accountability in financial-access services.

Proposed executive benefit: Contribute a concrete approach to agent safety and risk acceptance.

What This Recruit Could Add to ISA

Show an AI-agent release case with data tiers, tested behavior and retained human authority. **Source:** www.theregister.com

Handbook connection: Tool E 48-50; K 66-68. 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

Industry advocacy / collaboration: Own collective-defense endorsements and joint public letters; these are advocacy signals, not sole authorship or testimony.

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.strausscenter.org

Company mark: Current employer website brand asset Source: block.xyz

Attributable commentary and evidence ledger

10 / 10 substantive sightings recorded. Depth target met.

1. Block red-teamed its own AI agent to run an infostealer

January 12, 2026 | Direct attributed interview [Source: www.theregister.com](https://www.theregister.com)

Describes red-teaming an internal AI agent and requiring evidence that agent behavior is safer than the human activity it replaces.

Attribution / limitation: Company experiment is self-reported; no independent assurance of general safety.

2. D@S #75 - The Bigger Risk Is Refusing to Adopt AI Agents At All

February 11, 2026 | Direct podcast interview; publisher summary [Source: www.detectionatscale.com](https://www.detectionatscale.com)

Discusses data sensitivity tiers, human review and bounded AI deployment in detection engineering.

Attribution / limitation: One interview counted once, including its syndicated clips. Reported performance metrics are not independently verified.

3. Cybersecurity is moving from IT function to economic foundation - The Irish Times

July 3, 2026 | Direct attributed comments [Source: www.irishtimes.com](https://www.irishtimes.com)

Describes AI being used across phishing, data theft and extortion. Says coding agents mix instructions and data unpredictably, can be manipulated through natural-language context and have opaque, difficult-to-test failure modes.

Attribution / limitation: Only Nettesheim's attributed remarks are used, not other speakers' workforce or policy arguments.

4. ChromeOS makes security simple for Block

May 1, 2024 | Coauthored customer case with Matthew Solly [Source: cloud.google.com](https://cloud.google.com)

The coauthors describe centrally managed outsourced-support endpoints, rapid provisioning and device posture checks linked to identity. Nettesheim's separately attributed comment connects trusted device signals to secure application access with little user friction.

Attribution / limitation: A joint Block customer case hosted by Google; deployment and benefit claims are self-reported. Do not treat all text as Nettesheim alone or the named products as an ISA recommendation.

5. Using Santa To Augment Forensic Investigations

DFRWS EU 2018; transcript published February 4, 2019 | Joint technical presentation; speaker-labeled transcript [Source: www.forensicrofocus.com](https://www.forensicrofocus.com)

In his labeled passages, Nettesheim explains application execution controls, logging and enterprise-wide searches. Discusses the tradeoff between user-driven approvals and administrative review, including thresholds and monitoring; recognizes that the control can be bypassed.

Attribution / limitation: Historical Google presentation with Gary Brown; only James-labeled passages are attributed to Nettesheim. Transcript has bracketed uncertain words. Neither presenter claims to have developed Santa; no current Block deployment is inferred.

6. AI and financial security: Block's FSOC contribution

2026; issuer page undated | Own attributed quote plus employer context [Source: block.xyz](#)

Nettesheim describes using AI to analyze signals at scale and detect unusual patterns proactively to prevent fraud and financial crime before customers are harmed.

Attribution / limitation: His own quote supports proactive detection; production-review, monitoring and vendor-contract details elsewhere on the page are company context. Results are self-reported, not independently audited. The related LinkedIn post counts as the same event.

7. Reuters Momentum AI keynote - explainability and secure design

2025; exact recording date unverified | Attributed host keynote summary shared by Block [Source: www.linkedin.com](#)

The host summary attributes to Nettesheim a focus on explainability, secure design and risks from prompt injection, deepfakes and adversarial AI.

Attribution / limitation: Publisher summary, not a reviewed transcript. Lucas Kello's separate keynote is excluded; no legal requirement or detailed implementation claim is inferred.

8. Own public hiring post: security across engineering and product boundaries

Posting date unverified; reviewed October 11, 2026 | Own LinkedIn hiring commentary; indexed public text [Source: www.linkedin.com](#)

In a principal-security-engineer hiring post, he describes hands-on security leadership spanning engineering and information security, shaping product and infrastructure architecture so secure design supports innovation.

Attribution / limitation: Own post text reviewed through the publicly indexed profile. Direct post permalink and exact date were not recoverable. This expresses hiring priorities, not a measured program outcome or an ISA commitment.

9. Own support for collective cyber defense

2026; exact post date unverified | Own LinkedIn endorsement plus primary signatory list [Source: openai.com](#)

His own public post welcomes Block joining a collective cyber-defense call and urges a coordinated response. The primary letter independently lists Block among its organizational signatories.

Attribution / limitation: Short personal endorsement; detailed technical recommendations belong to the collective letter, not Nettesheim alone. Organizational signatory status does not prove his personal authorship or an ISA partnership.

10. Signatory: replace outdated security advice with practical safeguards

November 24, 2025 letter; own post date unverified | Joint open letter and own public endorsement [Source: www.hacklore.org](#)

The letter he signed urges practical, proportionate guidance, phishing-resistant authentication, easy escalation and systems designed to withstand human mistakes. His own post endorses replacing folklore with useful advice for people and small businesses.

Attribution / limitation: His name and role are verified on the primary signatory list; this is a joint position, not sole authorship. Audience is everyday users and small businesses, not every high-risk threat model.