



#1

Summer Craze Fowler

Corporate Vice President and Principal
Exponent

Current employer biography confirms the role and Philadelphia office; Torc and Motional roles are historical. [Current-role source](#)

Public business email: sfowler@exponent.com | **Office:** +1-215-594-8855

Public contact source. Named public professional route; delivery/access and personal response are not confirmed. [Source:](#) www.exponent.com

LinkedIn profile | **Named professional biography / public route**

Work base: Philadelphia office listed by employer. Employer-listed office; residence and travel availability unconfirmed.

Recommendation and rationale

First-group qualification. ISA introduction lead; enterprise/scientific operating leadership, testimony, metrics and resilience expertise.

Research rank #1 - ISA core recommendations. Final research recommendation for this pass; ISA selection and outreach approval pending.

Company capacity and proposed benefit

FY2025 total revenue \$582.0m (\$536.8m before reimbursements); net income \$106.0m; 1,212 employees at January 2, 2026. Listed engineering and scientific consultancy. Annual \$75,000 corporate sponsorship is approximately 0.013% of FY2025 revenue (calculated), but interest and authorization are unconfirmed.

[Source:](#) investors.exponent.com

Proposed company benefit: More useful cyber-risk assessments and clearer evidence for investment and recovery decisions.

Proposed executive benefit: Access to directors and peers to test her metrics methods and inform practical oversight guidance.

What This Recruit Could Add to ISA

Create a dashboard linking engineering evidence, residual risk and investment outcomes. [Source:](#) www.ians.com

Handbook connection: Tool K 66-68; L 69-71. Proposed output and benefits require agreement. [Source:](#) www.nacdonline.org

Introduction and next decision

ISA-reported willing introducer; name not provided. Larry names Fowler as an introduction priority but does not identify the member. [Source: mail.google.com](mailto:mail.google.com)

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

Policy history and board-selection fit

Direct testimony: Written congressional testimony on mission-oriented cyber resilience.

January 2017 - Heinz College Makes Cybersecurity Recommendations That Washington Should Consider Now | Carnegie Mellon University's Heinz College. Advocates clearer cyber-law definitions, federal breach-notification consistency and privacy/security in product design. [Source: www.heinz.cmu.edu](http://www.heinz.cmu.edu)

Historical SEI position. These are policy proposals, not proven legislative outcomes.

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	ISA-reported willing introducer; name not provided. 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: Name-matched image on named public biography. [Source: www.exponent.com](http://www.exponent.com)

Company mark: Current employer website brand asset [Source: www.exponent.com](http://www.exponent.com)

Attributable commentary and evidence ledger

10 / 10 substantive sightings recorded. Depth target met.

1. Business outcomes should determine cybersecurity metrics

April 4, 2023 | Direct interview answers published by IANS; historical role descriptions. [Source: www.ians.com](http://www.ians.com)

Fowler identifies two failures: no shared metrics framework and weak translation into business outcomes. She recommends understanding company goals first, explaining outputs and outcomes, disclosing residual risks, and showing why money is being allocated to particular controls. Metrics should serve the audience rather than the security team.

Attribution / limitation: The direct answers are usable. The older Motional role in the article is historical; the current biography footer does not make the original interview new.

2. Operational consequences matter more than vulnerability counts alone

September 15, 2026 | Coauthored Exponent article; collective position. [Source: www.exponent.com](http://www.exponent.com)

The authors recommend starting with adverse operating conditions and tracing the systems, safeguards and operator actions that can produce or prevent them. Identical controller vulnerabilities can yield different consequences in different plants. They also question whether primary and backup systems share credentials, workstations or remote-access infrastructure.

Attribution / limitation: Fowler is one of five listed authors. Do not attribute every sentence exclusively to her. The findings concern water utilities; broader relevance is interpretation.

3. Baseline source

April 2, 2026 | Coauthored Exponent article; collective position. [Source: www.exponent.com](http://www.exponent.com)

The authors warn against restoring systems so quickly that logs or other evidence are overwritten. They recommend explicit response roles, recovery criteria and tested backups. Long-term resilience should include early threat modeling, updateability, software-dependency transparency, independent testing and postmarket monitoring.

Attribution / limitation: Fowler is one of four authors. These are shared published recommendations, not an isolated personal interview or proof of agreement with ISA.

4. Security culture should enable safe work and shared responsibility

November 12, 2021 | Direct answers in Living Security interview transcript. [Source: www.livingsecurity.com](http://www.livingsecurity.com)

Fowler describes embedding safety in job descriptions and everyday responsibility, using team-level cyber ambassadors and ongoing communication, and treating supplier assessment according to the importance of the product or service. She also identifies data access, third-party relationships and supply-chain integrity as concerns.

Attribution / limitation: Argo AI is the historical setting. The transcript identifies individual speakers; do not assign interviewer Drew Rose's observations to Fowler. This interview is counted once.

5. Social engineering needs policy, training and technical safeguards together

June 9, 2021; publisher shows update October 6, 2026 | Article attributed to Fowler by IANS; update authorship unspecified.
Source: www.ians.com

The article recommends measures across departments, including independent approval of elevated access, known-channel verification of changed bank instructions, a second approver for transfers, and social-engineering tests. Its premise is that human-centered attacks require policy and technology controls as well as training.

Attribution / limitation: The original author attribution is Fowler. IANS does not identify who made the 2026 changes or distinguish updated text; do not present all current wording as a fresh 2026 statement by her.

6. Assess cybersecurity spending against planned and actual performance

March 15, 2018 | Single-author SEI article. Source: www.sei.cmu.edu

Fowler proposes adapting earned-value concepts to compare spending, planned scope, actual events and successful handling. Her examples distinguish failed expenditure, accepted risk that materializes, unforeseen impact, residual risk averted and unnecessary spending. She presents the model as an invitation to develop better indicators.

Attribution / limitation: This is a proposed measurement approach, not proof that the metrics became a validated standard. The article's old spending and crime projections are not used.

7. Start cyber-risk analysis with mission impact and critical assets

July 25, 2018 | Written congressional testimony under Fowler's name. Source: docs.house.gov

Fowler argues that agencies must manage attack consequences as well as threats. She favors identifying mission objectives, critical services and assets before working backward to threats. Her resilience approach integrates security, continuity, disaster recovery and IT operations; she also identifies legacy IT and workforce gaps.

Attribution / limitation: Reviewed written testimony, especially pages 1-3. This establishes historical congressional participation and her position then; it does not establish present policy access or endorsement of current ISA legislation.

8. Enterprise risk leadership translates board goals into operational decisions

May 24, 2018 | SEI podcast transcript; Fowler and Ari Lightman have separate turns. Source: www.sei.cmu.edu

In her own answers, Fowler describes a chief risk officer who looks across operational units, translates board and executive goals into business-unit execution, monitors risk and reports decisions requiring leadership attention. She emphasizes operating within risk appetite and communication across different types of risk.

Attribution / limitation: The publication date is confirmed by the SEI episode listing. Pages 2-3 of the transcript distinguish her answers from Lightman's; this is not sole authorship of the whole conversation.

9. Prepare to adapt before disruption rather than only recovering afterward

February 27, 2017 | Single-author SEI article. Source: www.sei.cmu.edu

Fowler proposes organizations that anticipate disruption and adapt before it happens. She describes scenario exercises as an early capability and proposes expanding toward continuous exercises based on real-world indicators. The discussion builds on operational resilience while calling for more proactive adaptation.

Attribution / limitation: The article describes an emerging research direction in 2017. Do not recast its historical AI examples or aspirations as proof of modern agentic-AI capabilities.

10. Workforce development should combine role-specific training and applied exercises

PDF dated December 2016; SEI publication listing February 23, 2017 | Coauthored SEI report; collective project account. [Source: www.sei.cmu.edu](http://www.sei.cmu.edu)

The report documents a USPS-SEI academy pilot with management and technical tracks, virtual and in-person learning, mentorship and tailored capstone exercises. It describes training existing staff and a two-year postgraduation service commitment. The paper addresses workforce needs revealed by a breach.

Attribution / limitation: Fowler is one of four authors. The report PDF title/date differ from the library listing. USPS's CISO Academy is distinct from ISA's proposed Virtual Cyber Academy; this does not prove support for ISA's model.

Prior ISA webinar engagement - supplied roster

Matched in ISA Webinar Attendees.xlsx, attendees.csv, row 288. Exact LinkedIn URL and supplied name/title reviewed; categorized FINAL v3 and v5 corroborate the row.

Supplied title: Corporate VP and Cybersecurity Principal | Brentwood Bank Board Member | The Forte Group Member | IANS Faculty | Co-host on Business Security Weekly Podcast

Supplied organization: Blank; current employer assessed separately. Registration does not establish current ISA membership, sponsorship interest or event attendance.

Individual webinar dates, repeat registrations, attendance and questions are not included in this source. Not counted toward ten substantive sightings.