# Discussion Topics & Conversation Starters

Securing Connected Operations: Where Physical and Cyber Risk Converge

*Ortus Club Roundtable Dinner · Nine-Ten, San Diego · Thursday, June 25, 18:30 PT*

**Moderator: Tracy R. Reed — Director of Security Practice / Cybersecurity Architect, Unrisk**

## The Group

Function runs across physical security, facilities, risk and compliance, and cyber/IT — spanning biotech, banking, defense, and tech. Three rough clusters worth playing off each other:

- Physical security & facilities — Dexcom, GenMark, Fate Therapeutics, Quick Quack.
- Risk, compliance & regulated industry — East West Banking, Wells Fargo, U.S. Dept. of War.
- Cyber, IT & digital — Papa, Zscaler, Axway, Snap, BD, SAIC.

| Organization | Title |
|---|---|
| **Quick Quack Car Wash** | Regional Leader, Operations |
| **Dexcom** | Sr. Manager, Global Security Operations & Protective Services |
| **BD** | Director, Digital Transformation |
| **Wells Fargo Bank N.A.** | EVP / Sr. Director, Product & Digital Innovation |
| **East West Banking** | Deputy Director, Risk Governance & Strategy |
| **Fate Therapeutics** | AD, Facilities Operations & Engineering |
| **Papa** | Chief Information Officer |
| **U.S. Department of War** | Program Director (Safety, Risk Mgmt, Operations) |
| **SAIC** | Senior Principal, LVC Wargaming & Training Ops / AI |
| **Snap Inc.** | Head of Security & Privacy, Snap Spectacles |
| **Axway** | VP, Center of Excellence for AI, Cloud & Security |
| **Zscaler** | Product Security, Customer Trust |
| **GenMark Diagnostics** | Director, EHS, Facilities & Security |

## Opening Round — Around the Table

**Let's go around the table: your name, your organization, and one part of your security operation where you wish you had a clearer picture than you do today.**

- If a few people name the same gap — who's on-site, who has access to data & systems, what happened after hours — flag it as something to come back to.

## Topic 1 — When Physical Meets Cyber

*Whether the convergence is real on the ground, or still just a slide.*

**Tell us about a time a physical problem turned into a cyber problem — or the other way around. When did that line actually blur for you?**

- Did it surprise you whose job it turned out to be?
- For the cyber and IT folks: when does a physical door, access badge, or on-premise visitor actually land on your desk?

## Topic 2 — The Scramble Before the Audit

*Being ready on any given day, not just the day you prepped for.*

**Think back to the last audit, inspection, or board ask you had to scramble for. What was the scramble actually like behind the scenes?**

- If an auditor walked in today and asked who was in your building last week, how long before you'd have a straight answer?
- What's the thing you quietly hope no one asks to see?
- For the regulated-industry folks: how does that change when it's a regulator asking, not just the board?

## Topic 3 — Piecing the Story Together

*The blind spots between physical security, access, and the digital systems meant to connect them.*

**Tell us about the last incident or investigation where you had to piece the story together from a bunch of different systems. Where did it fall apart?**

- When something happens on-site — a tailgated door, an after-hours entry, a contractor somewhere they shouldn't be — how confidently can you say who was where, and when?
- When an employee leaves your company, are you sure their physical access deactivates the same moment their login does? What about contractors?
- How much of what happens in the building actually reaches the systems your security team watches — and would you trust it if it did?

## Topic 4 — Falling Through the Cracks

*Coordinating across physical, IT, facilities, and compliance when they sit in different orgs.*

**Tell us about the last time something fell through the cracks between your physical and IT or security teams. What happened, and who ended up owning it?**

- Who gets the call first when an on-site incident might also be a data or privacy problem?
- Has anyone here actually merged or aligned these teams? How did that go — and what was harder than expected?

## Topic 5 — Compliant on Paper

*The gap between checking the box and actually being able to respond.*

**Can you share a time you were technically compliant — every box checked — but knew in your gut it wouldn't hold up if something real happened?**

- What would you actually need to be able to prove, and to whom, to feel genuinely ready?
- How do you show that to a board or auditors without it turning into a month of manual reporting every time?

## Topic 6 — If It Were Up to You

*Forward-looking, and an open round back to the table.*

**If budget weren't the obstacle, what's the one thing you'd fix in your security operations tomorrow — and what story would you have to tell to get it funded?**

- In a word or phrase: the biggest risk you're carrying into next year?
- If you could ask everyone at this table one honest question, what would it be?