QUIETCONVERSION

Does Cold Outreach Work in Cybersecurity?

Two Field Experiments. One Finding That Changes the Question.

BSides SF 2026 · RSA Conference 2026 · QuietConversion

101	48	100%	336+	~$10
BSides respondents	RSAC respondents	outbound participation	RSAC data points	total materials cost

Abstract

This paper presents findings from two sequential field experiments conducted at BSides SF 2026 and RSA Conference 2026. Together they address a question that generates strong opinions and weak data in the cybersecurity industry: does cold outreach work?

The short answer from 101 BSides respondents: 71% say no. But the more important answer — discovered in follow-up conversations with the 20% who said yes — is that cold outreach rarely converts through the mechanic itself. It converts through timing, and through an influence layer that most vendors are not deliberately targeting.

The RSA experiment then asked a deeper question: across seven GTM tactics, which break trust and which build it? The findings reveal a sharp and largely settled bifurcation, a contested middle worth understanding, and a persistent gap between what vendors know about their own tactics and what they continue to do.

Both experiments were conducted with hand-drawn foam board instruments, transparency sheets, colored dot stickers, and a five-year-old's stamp collection. Total materials cost: under $10.

Experiment 1: BScience · BSides SF 2026

INSTRUMENT	Hand-drawn trifold foam board. BSides-themed — BScience, with bee drawn as the “B”. YES / NO / MAYBE sections. Respondents stamped their answer using stamps from the researcher's son's collection. The BSides bingo game was running simultaneously; participants occasionally used the bingo stamps too, resulting in dolphins and giraffes appearing alongside flowers and eggs.
QUESTION	Have you bought anything from cold outreach in the last five years?
SAMPLE	n=101 respondents. All participants engaged through organic conversation first. 100% outbound engagement rate.

Results

Response	n	%	Signal
Yes	**20**	**20%**	Cold outreach did lead to a purchase — follow-up conversations reveal why
No	**72**	**71%**	Majority have not bought from cold outreach in five years
Maybe	**9**	**9%**	Uncertain — possibly indirect or timing-dependent
Total	**101**	100%	

Day 2 Addition: Do You Also Sell Cold?

On the second day, a respondent suggested tracking whether participants also sold via cold outreach. The researcher added this as a parallel track for remaining interactions.

Sells Cold?	n	%	Note
Yes	**14**	**50%**	Half of day 2 respondents sell via cold outreach
No	**12**	**43%**	
Maybe	**2**	**7%**	
Total	**28**	100%	*Unqualified by role — buyers and vendors mixed*

The gap is immediate: roughly half of this sample sells cold. Roughly 20% of the full sample has bought cold. Someone is wasting significant effort.

Finding: The Engineer Influence Layer

The most significant finding from the BSides experiment did not come from the board data. It came from follow-up conversations with the respondents themselves.

When asked what made them respond to cold outreach, the answer was fairly consistent: timing. They happened to be looking for that specific solution when the outreach arrived. The cold mechanic did not create the need or the interest — it arrived at the right moment.

This led to a deeper line of questioning about how purchasing decisions actually get made in cybersecurity. What emerged was a pattern that the standard cold outreach model does not account for.

> ***"I just buy whatever my engineer is bothering me about." — CEO, prominent security company, BSides SF 2026***

Multiple engineers described the same pattern: engineers identify a tool because they have a specific need, test it themselves, advocate internally, and eventually get budget approved by a manager or CISO who trusts their judgment. The CISO does not buy cold. They buy warm — warmed by their own team.

The engineer, meanwhile, does not buy anything. They test, recommend, and advocate. They are the influence layer through which cold interest is converted into warm decisions at the executive level.

What the industry targets	How decisions actually get made
Cold outreach to CISOs	Engineer has a need → tests a tool
Cold outreach to C-suite	Engineer advocates internally
Volume email sequences to senior buyers	CISO approves what their team already uses

Experiment 2: Break or Build · RSA Conference 2026

INSTRUMENT	Hand-drawn foam board designed to open like a folder, with transparency sheets on both sides to allow dry erase marker use and easy wiping between sessions. Inside left: respondent identifies role via colored dot (blue = buyer/influencer, red = vendor, green = investor, yellow = other). Inside right: break or build grid with 7 GTM categories and 4 response options (Break, Build, Maybe, N/A). Researcher placed stickers on respondent's behalf after confirming consent with first participant. QuietConversion mango logo on front cover. A research assistant was present for the first two days of data collection.
QUESTION	Do these categories break or build trust? [Evaluated across 7 GTM tactics]
SAMPLE	n=48 unique respondents (corrected after team review). 336+ total data points across 7 categories. Role composition: 14 buyers/influencers (blue), 23 vendors (red), 1 investor (green), 10 other (yellow).

Participation Methodology

All outbound participants were approached through organic conversation. No cold asks, no immediate survey request. Conversations began with open questions about the attendee's work and role. Participation was requested only when genuine engagement was established.

The researcher's outbound method — qualify first, build genuine connection, make the ask when timing is right — was the same set of principles being studied. The 100% outbound participation rate may reflect this congruence as much as any specific technique.

Participation by Channel

Channel	Approached	Participated	Rate	Notes
Outbound (researcher initiated)	44	44	**100%**	Every person approached participated
Inbound vendor	8	4	**50%**	2 participated without scanning. 2 scanned then refused.
Inbound other	1	0	**0%***	Self-identified as not ICP. Declined and continued organic conversation.

*Her continued engagement after declining is itself a qualitative note about conference relationship dynamics.

Results: The Trust Spectrum

Category	Break	Build	Maybe	N/A	Verdict
Cold Email	30 (63%)	7 (15%)	10 (21%)	1	**BREAKS TRUST**
LinkedIn DM	15 (31%)	22 (46%)	11 (23%)	0	**BUILDS TRUST**
Cold Call	37 (77%)	8 (17%)	2 (4%)	1	**BREAKS TRUST**
Warm Intro / Referral	2 (4%)	45 (94%)	1 (2%)	0	**BUILDS TRUST**
Dinner	5 (10%)	37 (77%)	5 (10%)	1	**BUILDS TRUST**
Thought Leadership	2 (4%)	39 (81%)	6 (13%)	1	**BUILDS TRUST**
Badge Scan / Booth Follow-up	9 (19%)	26 (54%)	10 (21%)	3	**BUILDS TRUST**

Role-segmented analysis shows broad agreement between buyers and vendors on the extremes: both groups rate Cold Call as breaking trust and Warm Intro as building it. The most notable divergence appears in warm tactics — vendors rated Dinner and Thought Leadership as building trust at significantly higher rates than buyers did. This gap between how vendors perceive their own warm tactics and how buyers experience them may warrant further investigation. Note: buyer sample size (n=14) limits the strength of role-segmented conclusions and these observations should be treated as directional rather than definitive.

1. Cold breaks. Warm builds. This is not close.

Warm Intro: 94% build. Cold Call: 77% break. These are not contested numbers. They represent settled perception across buyers and vendors alike.

2. Cold Call is the most settled signal in the dataset.

Cold Call received the highest break percentage of any category at 77% and also had the fewest maybe responses (4%), meaning people have largely decided. Cold calling in cybersecurity is not a contested tactic. It is a settled one.

3. LinkedIn DM is the only cold-adjacent tactic that net builds trust.

22 build vs 15 break (46% build). Every other cold tactic breaks more than it builds. LinkedIn DM doesn't. The 23% maybe rate suggests execution matters significantly — this is the most context-dependent cold tactic in the set.

4. Vendors know their cold tactics break trust. They do them anyway.

Vendors rated Cold Email as breaking trust at 57% and Cold Call at 70%. The gap is not in knowledge. It is in behavior.

> ***Vendors know cold outreach breaks trust. They're doing it anyway. That gap between knowledge and behavior is where the real GTM problem lives.***

5. The maybe column shows where execution matters most.

Category	Maybe (n)	Maybe (%)	Interpretation
LinkedIn DM	11	**23%**	High — execution dependent
Cold Email	10	**21%**	High — execution dependent
Badge Scan / Booth Follow-up	10	**21%**	High — execution dependent
Thought Leadership	6	13%	Moderate — context matters
Dinner	5	10%	Moderate — context matters
Cold Call	2	4%	Low — settled signal
Warm Intro / Referral	1	2%	Low — settled signal

Cross-Experiment Findings

The Cold Outreach Reality

Taken together, the two experiments paint a consistent picture. 71% of BSides respondents have not bought anything from cold outreach in five years. At RSA, Cold Email and Cold Call are the two highest-break categories. The finding is not that cold outreach never works — it's that it works far less often than vendors deploy it, and at a trust cost that is rarely accounted for in GTM strategy.

The 20% who said yes at BSides largely confirmed the same thing from a different angle: cold outreach didn't convert them because of the mechanic. It arrived at the right moment. Timing did the work.

A Note on Targeted Outreach

Several vendor respondents described a more sophisticated approach than volume cold outreach: monitoring prospects for significant events over time, building context slowly, then reaching out with a message tied to a specific relevant trigger. This methodology was described primarily by vendors with larger GTM operations and budgets. Whether it represents widespread practice or a minority of more sophisticated operators is unclear from this sample size.

Notably, this approach is not really cold outreach in the traditional sense — it is delayed warm outreach with a cold-looking surface. The 'cold' contact only happens after significant relationship groundwork. This may partially explain why LinkedIn DM performs differently from cold email in the break/build data: the platform is more compatible with this kind of monitored, triggered methodology.

For early and mid-stage companies without the resources to sustain this level of prospect monitoring, the practical implication of both experiments points in the same direction: community presence, thought leadership, and engineer-level relationships may offer a more accessible path than cold outreach at any sophistication level.

> ***Cold outreach doesn't convert through the mechanic. It converts through timing. Most vendors are optimizing for the wrong variable.***

The Engineer Influence Layer

The standard cybersecurity GTM model targets CISOs and C-suite buyers with cold outreach. But the BSides conversations revealed that these buyers often don't make purchasing decisions through cold channels at all. They buy what their engineers recommend.

This creates an influence layer that most GTM strategies are not deliberately targeting. The engineer tests the tool. The engineer advocates. The executive approves. The cold outreach to the CISO is either bypassed entirely or arrives after the decision has already been shaped from below.

Whether deliberately targeting engineers as the influence layer would outperform cold CISO outreach is a hypothesis this research opens but cannot yet test.

The Researcher as Instrument

Both experiments achieved high participation rates through organic conversation before any ask. At BSides, 100% engagement on a one-question survey with 101 respondents. At RSAC, 100% outbound participation across 44 outbound approaches.

These rates likely reflect a researcher effect — the researcher's approachability, conversational skill, and non-threatening presence reduced friction in ways that may not generalize to all researchers. This is a known phenomenon in field research and should be considered when interpreting participation data.

However, the participation pattern itself is a finding: the same principles the data endorses (qualify first, build genuine connection, make the ask when timing is right) are the principles that produced the data.

Limitations & Future Research

Both experiments were conducted by a single researcher at two conferences over six combined days and with an assistant for two of those days. Sample sizes (n=101 and n=48) are sufficient for directional findings but not statistical generalization.

BSides respondents were not segmented by role. The buying question was answered by a mixed population. Future iterations should add role identification.

RSAC role identification was self-reported. The sample skews vendor-heavy (23 of 48 identified as vendors), which may affect role-segmented findings.

The participation tracking board was a physical wipe-off surface.. Counts were tallied and updated after team review. Final counts reflect the best available data from field conditions.

All evaluated companies self-selected into conference participation, which requires financial investment. Sample reflects companies with sufficient resources to exhibit at RSA Conference 2026, not the full early-stage cybersecurity landscape.

Future research directions: deliberate engineer-targeting as a GTM strategy vs CISO-first; LinkedIn DM effectiveness by seniority and industry; timing as the operative variable in cold outreach conversion; cross-vertical comparison in fintech and healthtech.

About This Research

QuietConversion studies trust signals in cybersecurity go-to-market. This two-experiment paper is part of ongoing field research into how trust develops, breaks, and compounds across the full GTM stack — booth, website, drip, and beyond — with a focus on early and mid-stage companies in high-trust verticals.

These experiments were conducted alongside the QuietConversion High-Trust Booth Diagnostic (RSAC 2026), a separate instrument evaluating 13 trust signals across 60+ named booth interactions at the same conference.

The BScience board was made from a foam board trifold, markers, and stamps from a five-year-old's collection. The Break or Build board was made from a foam board folder, markers, a printed mango logo, and colored dot stickers. Total materials cost for both instruments: under $10.

The researcher is an independent cybersecurity GTM researcher based in the SF Bay Area.

Full methodology available upon request. Case studies from the RSAC 2026 booth diagnostic available at quietconversion.com.

Strategy matters.
But trust moves markets.

With heart,
— Rhea Lynn Mascarinas Founder & Lead Researcher | QuietConversion