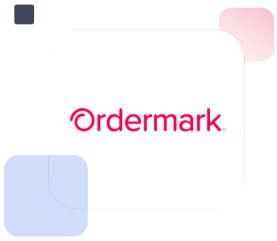
CASE STUDY

Ordermark Built To Last With Cybersecurity Awareness As Foundation



About

Headquarters: Los Angeles, CA and Denver, CO

Industry: Food delivery/restaurant tech

Size: 300 employees and rapidly growing

Challenge

Entering a phase of explosive growth, Ordermark knew its attack surface would expand along with its headcount and operations, jumping from 60 employees to over 300 in

Solution

Hoxhunt's focus on being people-first and creating a positive security culture got immediate C-suite buy-in. While measurably enhancing

under a year. Security posture is an increasingly important competitive advantage in their industry, where breaches can disrupt extensive supply chain networks of interconnected software vendors, commercial kitchens, and delivery platforms. Moreover, corporate culture is particularly important for attracting and retaining top talent, and traditional awareness tools often damage culture and are seen as disruptive to business operations.

awareness and significantly reducing risk of phishing breaches, Hoxhunt helped Ordermark meet compliance standards, establish a strong security culture, and elevate the infosec team.

Why this startup made awareness training a foundation of their growth and scale phase

And how they succeeded

“Right away our CTO was very supportive of Hoxhunt for its gamification aspect and as a way of keeping people aware without shaming them. And

our CEO was very supportive as well. He actually sent me a thank-you email for starting this program, which was just amazing. We have had such a great response. Almost 6 months into it, we have seen a **fail rate that was about 18% down to 5%,** even with simulated threat emails that are more targeted and complicated than they were initially. We are very happy with the results. The goal is to keep people aware that you've got to be careful with every email you receive, and I think Hoxhunt is achieving this very well." – Yves Accad, Director of Infrastructure and Security, Ordermark

Results

- **Measurably lower risk**: In under 6 months, threat simulation fail rate dropped from 18% to 5%, a 72% reduction related to risk of breaches, despite increasingly challenging threat simulations (as per design)
- **High participation**: Active engagement rate sustained at 80% throughout rapid corporate growth (from 60 to 300 employees)
- **Meaningful results**: Over 30 different, targeted threat simulations / employee / year makes pass/fail and engagement rates truly meaningful
- **True risk of a breach:** better known with high engagement-driven metrics
- **Buy-in from executive leadership and employees**: awareness is a watercooler topic and infosec team lauded in CTO/CEO's company standup presentations
- **Interdepartmental cooperation**: Top-performing employees get "sushi-points" from a joint HR-Infosec awards program
- Helped infosec team **build interdepartmental relationships** that have enabled security-positive decisions throughout growth
- Helps meet cybersecurity certification and auditing **standards**

Background: Why Hoxhunt?

Awareness training was the top priority for Yves Accad as the new Director of Infrastructure and Security at Ordermark set about designing a security system that could support the startup's rapidly accelerating growth. He'd identified email breaches as the biggest security threat over his 25 years in information security, and the problem had multiplied over the pandemic. But traditional awareness programs were ineffective: their 1-2 simulations and dry presentations per year offered weak results and hurt security culture. Management agreed. They wanted something different. A training program that would actually promote culture and long-term engagement.

After researching alternatives, he selected Hoxhunt, with leadership support, for its:

- **Customization**: Targeted threat simulations matched with individuals' skill levels and progress over time.
- **Gamification**

- **Ongoing cadence**: frequent threat simulations and micro-trainings to keep security front-of-mind
- **Automation**
- **Supportive learning**: simulation failures were followed by immediate micro-trainings, rather than some kind of punishment
- **Quality of content**: simulations stay current with the threat landscape, are challenging to spot, and hard to anticipate
- **Positive tone**: Encouragement supports learning better than punishment

Success metrics

Engagement rates have been sustained at over 80% even with rapid headcount growth. Globally, Hoxhunt data suggests engagement levels of around 70% are outstanding predictors of risk reduction and awareness; over 80% is excellent. That means that 4/5 Ordermark employees are actively participating in threat simulations calibrated to their improving skill levels, and they are also reporting real threats via the Hoxhunt button. In doing so, they remove those threats from the system. Ordermark notes that even employees who fail simulations participate in the follow-up mini-trainings. Overall, simulation fail-rates have dropped from 18% to 5% in half a year, even with high active engagement with dynamic simulations designed to get harder as employees' skill level increases.

Awareness and cybersecurity as a foundation for business growth

Ordermark noted that every new hire constitutes an enlarged attack surface. Along with their hundreds of new hires in 6 months, there's been expanded infrastructure: new vendors, new SaaS applications, and new contractors. Yves has been pleasantly surprised with how well the Hoxhunt awareness program has kept security front-of-mind, to where different departments request his input on how to approach expansion and operations in a secure manner.

"Relationships are one of the most important pillars of good security. A good security team cannot effectively secure everything. You cannot be in that ivory tower. Hoxhunt has helped us build those relationships with the different teams, where there's the communication and transparency that support the mutual desire to work together for the same cause, which is the success of our business. And securing our data is good for our business."

Awareness as a business advantage

Partnering with an increasing number of enterprise clients, Ordermark must demonstrate compliance with certain security standards. Awareness training helps with security audits and prove they are following security standards. Awareness training is part of virtually every security assessment (such as SOC 2 and ISO 27001) as it helps prove companies are equipping employees with the necessary skills to keep data secure.

Leadership is key

> ***"When Yves initially told me about Hoxhunt's approach to awareness training, it immediately resonated. Awareness training has historically been a "check the box" exercise organizations periodically go through, rather than continuous reinforcement blended in with daily activities of employees. Additionally, Hoxhunt's gamification approach aligned nicely with our internal recognition program to promote further engagement and excitement with employees." --*** **Arpan Desai, CTO, Ordermark**

What does executive buy-in look like? Aside from an enthusiastic thumbs-up for launching the Hoxhunt program, the CTO once shared with the company that even he had fallen for a Hoxhunt threat simulation. That showed how anyone is susceptible to an attack and thus everyone should care about information security. The CEO echoed that level support, and the HR department has incorporated information security into its employee rewards program, awarding top Hoxhunt performers each month with Ordermark “sushi points,” which can be converted to gift cards, food, or charitable donations. (The sushi point system existed before Hoxhunt, so as great of a metaphor as turning phishing emails into sushi is… it’s purely coincidental).

“The biggest key to success has been the support of our CTO and CEO. You need support from management so that people understand that cybersecurity is something to be taken seriously. At the end of the day, security starts from the bottom up. It’s a shared responsibility. But management has to demonstrate that security is important.”