NO BLIND SPOTS, NO CLICKS: LAUREL VALIDATES ITS ATTACK SURFACE AND HUMAN DEFENSES

CUSTOMER SNAPSHOT

laurel

INDUSTRY	Technology – Software & Services
CUSTOMER	Laurel is the work intelligence platform that automatically captures billable work for professional services firms, including major law firms and Big Four accounting practices.
SERVICES PROVIDED	Continuous Threat Exposure Management, Social Engineering

"You can buy all the security tools in the world, but that alone doesn't mean you're secure. The real question is whether your controls hold up when they're actually tested. That's what this engagement gave us—the opportunity to validate our defenses under real-world conditions."

— **ANTHONY LAUDERDALE, HEAD OF TRUST, LAUREL**

CUSTOMER OVERVIEW

Laurel is the work intelligence platform for professional services firms. AI handles capture, classification, and narrative drafting, automating the administrative work draining professional time and turning every work activity into ready-to-review timesheets, real-time profitability, AI ROI, and pricing intelligence. Its customer base includes major law firms, Big Four accounting practices, and organizations with the highest expectations for data privacy, security governance, and regulatory compliance.

That client profile raises the stakes considerably. When the firms trusting Laurel with sensitive billing data are themselves subject to rigorous security scrutiny, Laurel's own security posture becomes a direct business asset. Security questionnaires, trust portals, and vendor reviews are routine parts of doing business, and the ability to answer them quickly, confidently, and with evidence makes a meaningful difference.

When Head of Trust Anthony Lauderdale joined Laurel, he immediately set about building a mature, defense-in-depth program from the ground up. With a background that began in the FBI doing early threat intelligence work, Lauderdale brought a practitioner's mindset to the role: understand your adversaries, map your controls to their techniques, and practice the way you intend to play. By the time Laurel engaged Bishop Fox, the security program was in a strong place, but strong wasn't the same as validated.

THE CHALLENGE

Laurel invested deliberately in building its security stack. The organization had deployed endpoint detection, cloud security, threat detection, code security, email security controls, and more. Application penetration tests conducted bi-annually. Phishing simulations ran continuously. On paper, the program was comprehensive. What it lacked was continuous, adversarial-tested proof.

Point-in-time assessments could confirm that controls were configured correctly on a given day, but they couldn't answer the question Laurel cared most about: what was emerging between tests, and how would its people perform under real adversarial pressure? And with a growing customer base of security-conscious law firms and accounting practices, the ability to demonstrate that resilience (not just claim it) was becoming increasingly important.

SECURITY CHALLENGES

- **Continuous Visibility:** Periodic pen tests leave windows between assessments where new exposures could emerge undetected.
- **Emerging Threat Response:** With a fast-changing threat landscape, the team needs real-time intelligence on whether newly disclosed vulnerabilities applied to their environment.
- **Human Layer Validation:** Phishing simulations can lack the sophistication to replicate real-world social engineering tactics.
- **Stakeholder Confidence:** Enterprise customers expect Laurel to answer security questionnaires with evidence, not assertions.
- **Scalable Security Culture:** As the company grew past 150 employees, Laurel needs assurance that onboarding processes are instilling security awareness from day one.

"The proof is really in the pudding. We felt like we were in a strong place from a security perspective, but bringing in an experienced third party to validate that independently is what really matters."

— **ANTHONY LAUDERDALE, HEAD OF TRUST, LAUREL**

THE SOLUTION

While at a previous company, Lauderdale had engaged Bishop Fox to validate security controls during a period of intense public scrutiny, and the work had been exceptional. When he joined Laurel and began evaluating offensive security partners, the choice was straightforward.

The engagement began with a comprehensive scoping session. Laurel initially scoped an external penetration test, but early discussions with the Bishop Fox team led to a different starting point: continuous testing of their attack surface, powered by Bishop Fox's Cosmos platform. Given the maturity of Laurel's existing controls, the team recommended establishing a continuous baseline first by identifying any low-hanging fruit before moving to deeper adversarial testing. That recommendation proved sound. Over nine months of continuous monitoring, Cosmos surfaced only a single low-severity finding, proving that Laurel's external posture was genuinely strong. Alongside the attack surface testing, Laurel commissioned a social engineering assessment. Bishop Fox spent three weeks conducting a multi-vector campaign targeting nearly 50 Laurel employees, selected based on role, access level, and the likelihood of achieving the engagement's objectives. The campaign included phishing emails and text-based lures, crafted with the depth of research and operational tradecraft that distinguishes a real adversary from a simulation tool.

Bishop Fox consultants built out domains, conducted open-source reconnaissance on the company and its employees, and tailored the engagement to mirror genuine attack scenarios, including referencing a recent company offsite that had been publicly visible.

Throughout the engagement, Bishop Fox worked closely with the Laurel team, maintaining clear communication channels and providing real-time transparency into what was being attempted and why.

GOALS OF THE ENGAGEMENT

- Establish continuous visibility into Laurel's external attack surface and validate the absence of high-risk exposures
- Provide real-time emerging threat intelligence mapped to Laurel's specific environment and technology stack
- Conduct a sophisticated, multi-vector social engineering campaign targeting employees across levels and tenure
- Test whether technical controls (including identity, MFA, and domain monitoring) would detect and block malicious activity in real time
- Validate that Laurel's security culture would produce consistent reporting behavior, not just click avoidance
- Generate evidence-based reporting Laurel could use with enterprise customers and in compliance reviews

> "When you look at the top tier of red team and penetration testing firms, Bishop Fox is consistently in that conversation. I've seen the quality of their work firsthand throughout my career, so when I joined Laurel, the decision to work with them was an easy one."
>
> — **ANTHONY LAUDERDALE, HEAD OF TRUST, LAUREL**

THE OUTCOME

The engagement produced results that exceeded expectations on every dimension and provided Laurel concrete, reportable evidence of security maturity that no internal tool could have generated on its own.

KEY RESULTS

- **Zero Clicks Across 48 Employees:** Over three weeks of sustained phishing and smishing attempts against targeted employees (including a disproportionate share of newer hires, who are typically most vulnerable), not a single employee clicked a malicious link. This outcome is rare even among security-mature organizations running sophisticated campaigns.
- **Identity Controls Performed in Real Time:** Bishop Fox operatives created attack infrastructure, including spoofed domains. Laurel's identity monitoring detected these domains as they came online and flagged them immediately—well before any employee interaction occurred. Two domains were identified and would have been reported to the registrar for takedown in a real incident. The social engineering engagement would have succeeded had those controls not functioned as designed.
- **Active Reporting Culture Confirmed:** Employees didn't just avoid clicking; they reported suspicious activity through internal channels in real time. Multiple employees flagged lures without prompting, demonstrating that Laurel's security culture had embedded reporting as a reflex, not a policy.
- **Strong External Security Posture:** Continuous external attack surface monitoring surfaced only one low-severity finding over nine months, confirming a strong external posture and clean baseline for ongoing monitoring.

- **Emerging Threat Intelligence Validated:** The emerging threats capability surfaced at least one relevant vulnerability during the engagement period. Laurel confirmed it had compensating controls already in place, enabling the team to respond confidently to the disclosure without scrambling. Lauderdale noted this capability gives him the ability to answer customer questionnaires on emerging threats immediately and with specificity, rather than asking for time to investigate.
- **Board-Ready Evidence:** The combined results of zero clicks, one low finding, active employee reporting gave Laurel's leadership clear, third-party-validated proof points for board presentations, trust portals, and enterprise customer security reviews. The results speak for themselves without exaggeration.

"I believe you practice how you play. Having a firm with the depth of experience and expertise that Bishop Fox brings spend weeks testing our organization through phishing simulations, text messages, emails, and other social engineering tactics—and seeing employees consistently report suspicious activity rather than engage with it—is a real testament to Laurel's security culture and the security awareness program we've built here."

— **ANTHONY LAUDERDALE, HEAD OF TRUST, LAUREL**

CONCLUSION

For Laurel, the Bishop Fox engagement was the capstone of a nearly three-year program-building effort, the moment the work was put to a real test by people who attack for a living. The results validated not just the tools and configurations Laurel had assembled, but the culture it had worked to build: a company where employees trust security, report without hesitation, and treat vigilance as a shared responsibility.

The story Laurel can now tell its customers is a compelling one. It's not a list of controls or a certification. It's evidence: a sophisticated, multi-week adversarial campaign conducted by one of the most respected offensive security firms in the industry—and the company held. That kind of proof is particularly meaningful in the legal and professional services markets, where trust is currency and security scrutiny is a standard part of every vendor relationship.

Looking ahead, Laurel plans to expand its offensive security program with a product-focused red team exercise, additional penetration tests at an increased cadence, and continued investment in the managed attack surface services. The foundation is strong. The goal now is to keep testing its limits.

"It's one thing to talk about security; it's another to speak about it confidently and back it up. When customers send security questionnaires, we're able to respond quickly with clear, confident answers because we know the controls, processes, and safeguards are truly in place."

— **ANTHONY LAUDERDALE, HEAD OF TRUST, LAUREL**