CASE STUDY

SaaS Tech Company Narrowly Avoids Social Engineering Scam

INDUSTRY
Technology

EVENT TYPE
Social Engineering

REVENUE
<500K

EMPLOYEE COUNT
1–25

LOCATION
Washington

KEY COVERAGE
- Breach Response

"I was thrilled. I originally bought this insurance policy to check a box, but it has provided a valuable service."

Lara Ferroni, CEO, Project 529

Project 529, a technology company that helps reduce bicycle theft, set up a bug bounty program (a deal offered by websites, organizations, and software developers where individuals can receive compensation for reporting bugs such as security exploits and vulnerabilities) to uncover flaws in its product. If a legitimate "bug" was reported, the company would fix the flaw and pay the reporting party for its assistance[1].

One day, the company was contacted by a group of "white hat" hackers who reported multiple vulnerabilities. The severity of the vulnerabilities was overstated but still legitimate, so Project 529 paid the group and fixed the flaws. That's when things escalated.

The group then reported a list of nearly 50 vulnerabilities. Project 529 reviewed the list and disagreed that they were valid or critical issues, despite the group's insistence that they were, but still offered a lump-sum payment for the entire list. The group refused the offer and demanded individual payments for each vulnerability: one was priced at $100,000 and another at $20,000.

Unsure of how to proceed, Project 529 CEO Lara Ferroni remembered her company had purchased cyber insurance[1] to comply with security requirements. When Ferroni pulled out her policy, she noticed that it said to report anything suspicious, even if the policyholder is uncertain about an issue. That's when she called Coalition.

Our claims team quickly set up a meeting with Ferroni the next day to gather all the facts. She spoke with a claims manager and a team member from our affiliate Coalition Incident Response (CIR)[2]. "I'm under quite a bit of stress, as you can imagine," Ferroni recalled saying. "We've been going back and forth, and the group keeps getting more and more threatening. I don't think it's legitimate, but you just never know, and we take security very seriously."

Immediately, CIR instructed Ferroni to cease all communication with the group while assuring her they'd do more research. "I was thrilled," Ferroni recalled. " I originally bought this insurance policy to check a box, but it has provided a valuable service. I finally got a good night's sleep right after that call."

Upon further investigation, CIR determined that the group was not only illegitimate but also using AI-generated images for its "employees." CIR also audited Project 529's IT infrastructure and provided recommendations to improve its overall cybersecurity posture, including locking one of its registered domains and adjusting its customer login design to protect against phishing attempts, but determined there were no breaches or critical security issues

Continued →

Ultimately, Project 529 paid its self-insured retention to trigger its Breach Response coverage. CIR's full investigation and an additional call with outside breach counsel about storing customer data were covered under the policy.

Lesson Learned: When in doubt, report suspicious behaviors

A sense of urgency and unexpected changes (like an increased payment demand) are both strong indicators of a scam.

Ferroni and her colleagues at Project 529 felt something was off about the scammers soon after paying the initial bug bounties. This incident underscores the importance of being cautious in digital communications. A sense of urgency and unexpected changes (like an increased payment demand) are both strong indicators of a scam. In this instance, the scam was attempted under the guise of the bug bounty program, but we often see these tactics in phishing attacks and other types of extortion.

"Cyber insurance is totally worth it even just for the peace of mind," said Ferroni. "Scams are happening more and more often. If you're a small or medium-sized company, you don't necessarily have the resources to handle an incident. If you have a serious vulnerability, that's potentially the end of your business. Having cyber insurance to back you up is really important."

We encourage all policyholders to immediately report suspicious behavior. Contacting Coalition as early as possible gives businesses the strongest chance of avoiding a claim altogether. With an average response time of five minutes, our in-house claims team takes immediate action to help businesses navigate the response and recovery process and help mitigate financial and operational losses due to cyber risk.

Coalition brings together active monitoring, incident response, and comprehensive cyber insurance designed to help mitigate your organization's cyber risk.
To learn more, visit coalitioninc.com.

[1] *The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.*

[2] *Breach response included the engagement of an incident response firm; the insured selected Coalition Incident Response.*