JENCAP®

CASE STUDY

HIDDEN SOCIAL ENGINEERING TRIGGER CLAUSE PUTS COFFEE FRANCHISE AT RISK FOR CLAIMS DENIAL

New cyber risks are developing at an alarming pace. Working with a cyber insurance expert keeps businesses on top of emerging cybersecurity threats and ensures their policies adequately cover current risks.

UNCOVERING HIDDEN TRIGGER CLAUSES

Not long ago, Jencap Managing Director Taras Shalay was approached by a retail agent to quote a very large coffee franchise with hundreds of locations. The agent was unfamiliar with cyber insurance coverage for a business of this size and wanted the support of an expert.

The coffee franchise's current policy had an insuring agreement for social engineering and didn't mention any limitations, other than a sub-limit of $250,000. On the surface, this all seemed very standard and common for the cyber marketplace, but as Shalay dug into the policy language, he noticed a red flag.

Buried deep within the policy form was an endorsement for social engineering with a very alarming trigger clause. In the event of a social engineering incident, the policy would only provide coverage if certain criteria were met.

In this case, the criteria were impossible to meet. We'll use an example to explain.

HOW SOCIAL ENGINEERING WORKS

Let's say a cybercriminal sends an email to an employee in the coffee franchise's accounting department. The email appears to be from the company's CEO and lets the accountant know that

one of the company's vendors needs to update their banking information. The message goes on to ask the accountant to wire funds using the new account numbers provided. The email seems authentic, so the accountant complies — and willingly transfers $100k directly into the cyber criminal's account.

The money is now gone, without any apparent element of theft.

In this scenario, the trigger clause in the coffee franchise's policy required the accountant to first verify the authenticity of the request with the CEO before wiring the funds. If they did not do that, the policy wouldn't cover the fraud.

Here's the problem: Had the accountant done this, the theft would have been averted, meaning the risk of social engineering would have been eliminated from the very beginning. This undermines the value of having a social engineering agreement in place to begin with.

THE MAIN CHALLENGE WITH COVERING CYBER RISKS

Cyber is unlike most other insurance lines of business. As a new and emerging market, cyber language and terminology is not standardized throughout the industry and can vary drastically from carrier to carrier. And because technology continues to evolve rapidly, the cyber risks and threats we'll experience five years from now are things we can't even imagine today.

Since this line of coverage is such a moving target, finding issues with policy language can be a challenge for even those familiar with cyber coverage. Fortunately, Shalay's extensive experience aided him in finding this trigger clause that left a coverage gap.

TARGETED MARKETING BEATS "BATCH AND BLAST"

After Shalay and the franchise's retail agent explained the policy gap to the company's board of directors, they began the process of finding an alternative carrier.

Many wholesale brokers take a scatter-shot approach to marketing an account; they shoot off applications to every carrier available to them. They do this out of fear they'll miss something or in an attempt to block other brokers and eliminate competition. But, as explained by Shalay, that's not an ideal situation and can ultimately damage the relationship with a carrier.

> *"Our team goes to great lengths to understand the underwriting guidelines for carriers, what their target risk looks like, and where they shine. When a client comes to us, we're able to submit to a few targeted markets on their behalf. Because of the trust we've built amongst carriers, we get the best terms, the best pricing, and the fastest response time.*

Shalay found a carrier that provided a cyber policy with much less restrictive terms. And on top of that, he leveraged the risk mitigation and security controls the coffee franchise already had in place to negotiate a reduced rate.

PARTNER WITH SPECIALTY WHOLESALERS WHO UNDERSTAND YOUR COVERAGE NEEDS

Shalay has worn many hats throughout his insurance career — from carrier underwriter to retail agent and now a wholesale broker specializing in cyber insurance. Pulling from his diverse background and experience, Shalay is uniquely positioned to understand how to best work with both his carrier and retail agent partners.

At the end of the day, Shalay knows firsthand how challenging and frustrating cyber insurance can be for a retail agent. "I once was an agent myself, and being a strong generalist is their forte. But as insurance has evolved, our retail partners have grown to rely on us to help protect their errors and omissions. We can guide them to the best products and coverage for their clients, without them having to memorize and compare policy language. They can trust us to help them navigate through this ever-changing landscape."

Taras Shalay

Midwest Region Managing Director of Jencap Insurance Services

Taras began his insurance career in 2007 as an underwriter for Philadelphia Insurance Company, where he and his team created and wrote one of the first monoline cyber policies in the standard market. His expertise includes Cyber, D&O, Professional, and Employment Practices Liability.