300 Cyber Security

THE TRAVELERS CASE

A CAUTIONARY TALE FOR ORGANIZATIONS IN 2022

www.300cybersecurity.com

300 Cyber Security

THE TRAVELLERS CASE

Cyber insurance. It's a necessary business component in the 2020s, but it didn't exist 25 years ago. It wasn't even that common until a decade ago, so in the insurance world, it's new. The market is still rapidly changing, attempting to keep pace with the constant advancements of technology. The summer of 2022 quietly marked a milestone that likely didn't land on your radar but will significantly alter your relationship with your cyber insurance policy moving forward.

In the cybersecurity industry, it's known as the Travelers Case. More formally, Travelers Property Casualty Company of America v. International Control Services Inc. (ICS), filed in the U.S. District Court for the Central District of Illinois (No. 22-cv-2145). It is the first time an insurer has filed suit against an insured company for making misleading statements on their cyber insurance application. The case settled out of court, with both parties agreeing the policy was void and would not cover losses sustained by a ransomware attack in May 2022.

300 Cyber Security

THE RISK OF BEING LESS THAN FULLY TRANPARENT

Why is that significant? It's the first case showing that the answers you provide on your cyber insurance questionnaire matter. I remember when questionnaires were simple one-pagers. It wasn't uncommon for executives to put a positive spin on questions they didn't understand, laughing it off as "probably true."

Insurers initially saw cyber as easy money and didn't seem to care all that much as long as policies were paid. Even as the questionnaires got more detailed, there was a tendency (or sometimes executive pressure) to be overly optimistic with the answers—a best-foot-forward approach from the insured's perspective.

The Travelers Case illustrates the perils of being less than fully transparent. The issue at the centre of the argument was multifactor authentication (MFA). The insured stated on the application they were using MFA, and they were, but just on the firewall. I would hazard to guess that when an insurance company asks if you are using MFA, they mean are you using it everywhere? The applicant, using MFA in one place only but is seeking a check box, answers in the affirmative. While technically correct, we all know they aren't talking about the same thing. In the Travelers Case the forensics investigation correctly concluded MFA was not in place to protect the network, and thus the policy would not cover losses sustained.

If you took an optimistic view on your cyber insurance application, you might not have cyber insurance.

This case illustrates the importance of clearing up any vagueness on the insurance application or in your answers. From a technical perspective, the insured should have known better, but without seeing the application, it's hard to know exactly how the question was asked. There can be little doubt the person who answered the question was taking a best-foot-forward approach.

What does this mean for your company? If you took an optimistic view on your cyber insurance application, you might not have cyber insurance. Don't panic. Your best course of action is to simply adopt the things you said you had in the first place. It's far more prudent to do so anyway.

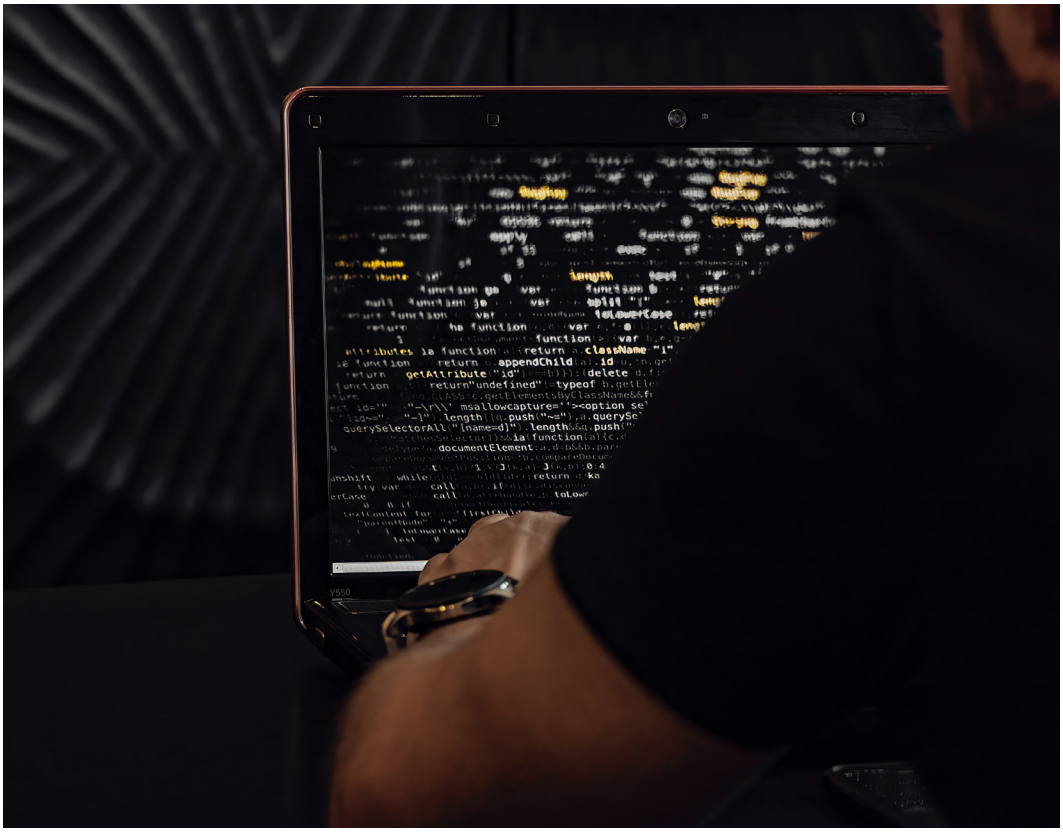
300 Cyber Security

REFRAME YOUR VIEW OF CYBER INSURANCE

Cyber insurance is no different than fire insurance. Yes- you need to have it. If your house burnt down, the money from the policy would build you a new house. But money cannot make up for the stress and disruption to your life. Also, there are things that cannot be easily replaced, and in some cases, when lives are lost, money doesn't matter.

An insurance payout doesn't easily replace things like reputation and customer trust. A decade of lost corporate knowledge cannot be regained. There are cases of attacks so damaging you can't put your business back together. You don't leave the house with a candle burning because you have fire insurance, nor should you live with known gaps in your cybersecurity because you have a cyber policy.

Adopting robust security procedures is far cheaper than putting the pieces back together after a cyber attack. But if you take all necessary precautions and your prudent defenses are still breached, you will know you have an insurance company behind you to help you through the disaster. However, enter into your relationship with the understanding the insurer could very well be looking for an "easy out" of their obligations should things go south. Please don't give them one.



300 Cyber Security

ABOUT 300 CYBERSECURITY INC.

300 Cybersecurity was born to allow sub-enterprise IT professionals to leverage best-in-class security tools, made for companies exactly like theirs, without having to turn over control of their environment to a third-party managed services provider.

We offer a comprehensive, tools-based cybersecurity solution for small internal IT teams managing organizations of 50-500 users. We install, configure, and support enterprise-grade security tools to create a holistic, 360-degree cyberdefense, thereby giving our clients a significant improvement in their security posture in a matter of days.

FOLLOW US

300-cybersecurity-inc

300_Cybersecurity

300-Cybersecurity

Dave Mason
President
300 Cybersecurity Inc.