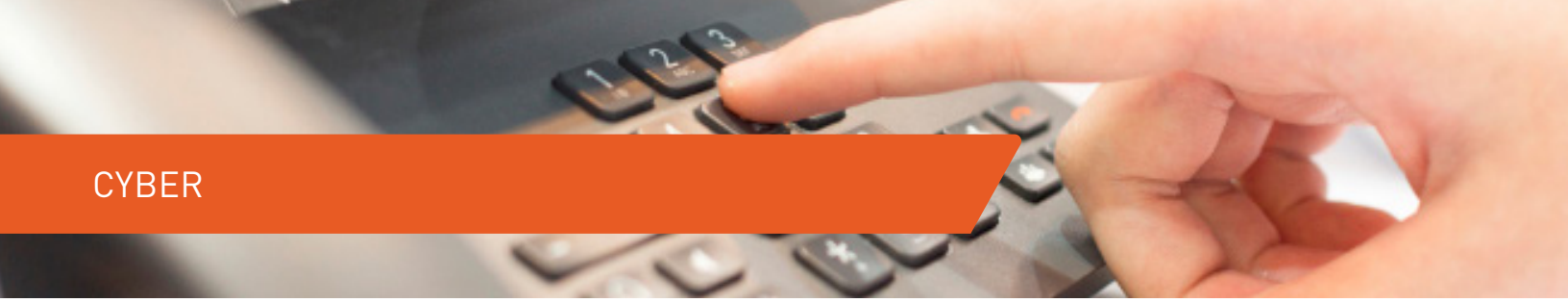

CYBER

Telephone Toll Fraud

Companies using VoIP telephone systems are at risk

VoIP telephone systems can be an attractive target for hackers. It starts when hackers lease their own premium-rate phone numbers, often used for chat or psychic lines, from a web-based service that charges dialers for each call and provides a cut of the money to the lessee. The hackers then breach a business' voice over IP (VoIP) phone network and forward calls through it to their own premium number. Using computer systems, they can make hundreds of calls simultaneously – forwarding the calls to the leased pay line. The hacker then gets a percentage of the pay line charges delivered to them through wire transfer. The company is then charged for each call routed through their VoIP system.

Often, a company is not aware of the hack until they receive an enormous bill from their phone provider. Telephone toll fraud affects mainly small businesses that use local phone carriers. Local phone carriers often lack the sophisticated anti-hack controls needed to prevent situations from occurring; leaving the hacked customer to pay the bill.

Claim Example

ABC Engineers was opening a new office location and decided on a VoIP telephone system to get better rates on international calls. The firm had several international projects and the VoIP system offered by their local telephone carrier had attractive rates on international calls.

Two months after opening their new location, a member of accounting alerted the office manager that a bill totaling $175,000 was received from their telephone carrier. Upon investigating the phone bill more closely, they discovered hundreds of calls placed on the last Saturday of the previous month. After confirming no one had been in the office to make the calls, ABC Engineers pressed their phone carrier to look into the issue. The phone carrier was able to determine ABC Engineers was a victim of telephone toll fraud. Hackers had breached their VoIP system and routed hundreds of phone calls through a premium 900 number. The phone carrier claimed ABC Engineers did not have strong internal controls in place and refused to let them out of the bill.

How Does the Victor Policy Respond?

Telephone fraud coverage is included in the Cybercrime Endorsement, an optional coverage under the Victor Cyber Policy.

Assuming ABC Engineers' VoIP system had basic security controls in place, including a system password that was changed every 45 days and disconnecting/disabling calls after entering an incorrect password three times, the fraudulent phone charges would be covered in excess of the deductible up to the limit of liability purchased.

Visit victorinsuranceus.com/cyber for more information or contact a Cyber underwriter at (301) 961-9800 or cyber.us@victorinsurance.com.

VICTOR