EPIC Insurance Brokers & Consultants

CYBERSECURITY

TELECOMMUNICATIONS FRAUD

WHAT IS TELECOMMUNICATIONS FRAUD?

In the digital age, phone systems are frequently interconnected with the corporate computer network, but often overlooked as a security vulnerability. Hackers can infiltrate phone systems via the customer's network or the telecommunications service provider. Once fraudsters have gained access, they then manipulate the phone system to make unauthorized long-distance calls leaving the customer with an exorbitant bill. Through staff awareness training, companies can take steps to mitigate or prevent such hacks.

TELECOMMUNICATION FRAUD TECHNIQUES

- **Provider Frauds**: These frauds are the most complicated because they infiltrate the service provider itself. These schemes create a behind-the-scenes fraudulent system that is invisible to the telecommunications service provider's customers but generates a large bill for the customer.
- **Customer Frauds**: This technique infiltrates companies who use telecommunications services. Hackers can enter into the phone network via voicemail system, improperly discarded SIM cards and pre-paid calling cards. After infiltration, the fraudster uses the phone system to make unauthorized calls, often to high-cost locations.

REDUCING THE RISK OF A TELECOMMUNICATIONS FRAUD LOSS

- Regularly monitor call activity to detect suspicious patterns
- Review phone bills fully to avoid overlooking fraudulent transactions
- Change voicemail passwords from default settings and do not use ones which can be easily guessed such as 1-2-3-4 or 0-0-0-0.
- Report lost or stolen phone equipment to the service provider to prevent manipulation by hackers.
- Develop corporate-wide awareness for telecommunications fraud through corporate culture, education and training.

DID YOU KNOW?

Global losses due to telecommunications fraud amount to about $32.7 billion annually.[1]

Nearly 5% of voice mail passwords are 1-2-3-4. The next most frequently used password is 0-0-0-0.

CLAIM EXAMPLE

An unauthorized third party gains access to an insured's telephone system, using it to incur $50,000 in international call charges. The insured only discovers the loss when it receives its monthly statement from the telecommunications service provider containing the fraudulent charges.

[1]OCCRP 2019, Report: US$32.7 Billion Lost in Telecom Fraud Annually, 22 March 2019, https://www.occrp.org/en/daily/9436-report-us-32-7-billion-lost-in-telecom-fraud-annually

EPIC
Insurance Brokers & Consultants

CYBERSECURITY

TELECOMMUNICATIONS FRAUD

INSURANCE SOLUTIONS FOR TELECOMMUNICATIONS FRAUD

CYBER COVERAGE

Cyber risk mitigation involves taking proactive steps to protect against and reduce the adverse effects of the key risks to your organization. Implementing network security defenses, incident response plans and employee training are all essential elements of cyber risk mitigation. Unfortunately, this is not enough. The reality is, no organization is immune from a cyber-attack, regardless of the strength of their defenses. This is where insurance can help. Comprehensive stand-alone cyber insurance will help protect the organization's balance sheet by transferring some of the costs associated with the inevitable breach.

Cyber insurance complements and supports active security measures by providing third-party regulatory and liability coverage as well as a host of first-party response, remediation and recovery insurance. In addition, most cyber markets also provide free or discounted pre-loss services to assist an organization in breach preparedness.

RISK MANAGEMENT TIPS

- Develop a written incident response plan that includes IT, HR, Accounting Staff, Security and Management
- Appoint a Computer Information Security Officer
- Identify, contain and protect any Personally Identifiable Data
- Continually maintain and upgrade computer systems and software
- Implement mandatory employee training to better prevent phishing, unauthorized transfer of funds, or unwitting data breach
- Encrypt all mobile devices
- Contact your VoIP provider to discuss security measures

CRIME COVERAGE

Commercial Crime insurance provides first-party coverage intended to help an organization recoup losses due to employee dishonesty, theft of money or securities, robbery, burglary, forgery and alteration, and theft of client property. In addition, Commercial Crime policies also typically include coverage for Computer Fraud, Wire Transfer Fraud and Social Engineering Fraud. Today, many stand-alone cyber policies also include similar or identical coverage extensions. This means there is a potential for overlapping and/or redundant coverage. Organizations should strive to coordinate coverage between stand-alone cyber and crime policies in order to ensure they are able to maximize potential insurance recoveries in the event of an incident.

In addition to the above, most commercial crime policies also provide a limit for investigation costs for covered loss, assisting the insured in paying for the complex process of determining the extent of the loss once the fraud has been uncovered. Coverage is typically on a loss discovered basis, meaning that the cumulative loss over time, regardless of when it took place, is covered by the policy in place when the loss is discovered.

RISK MANAGEMENT TIPS

- Establish an anti-fraud policy and code of conduct, with a hotline for employees to call if they suspect fraudulent activity. Conduct anti-fraud training and procedures for employees, managers and executives
- Conducting external audits of internal controls used in financial reporting
- Maintain multi-person controls in accounting and inventory
- Vet, update and purge approved vendor lists at least annually