Cyber Deception/Social Engineering

What is Cyber Deception?

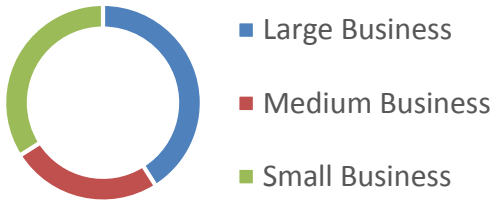
Cyber Deception, which is also called *Spear-Phishing* or *Social Engineering*, is a complex *cyber crime* designed to gain access to your funds by circumventing your firm's existing controls. These crimes, which are meticulously planned, usually involve tricking unsuspecting individuals into transferring money or information directly to the social engineer. These cyber thieves monitor email, websites, and the social media of both you and your contacts to gather information about your firm and your employees. They then impersonate an employee, friend, client or vendor of your firm, in a series of authentic looking emails. Once the scam is discovered, it is often too late to recover the lost funds.

Is Your Company Safe from a Cyber Deception Attack?

Cyber Deception is an increasingly common phenomenon, affecting businesses of all types and sizes. A one-person real estate or accounting office is just as likely to be a victim of cyber deception, as a "brand name" company with thousands of employees. According to a recent report by security risk management firm Hillard Heintze, there are over 100,000 deception fraud attacks each day.[1]

Cyber thieves typically exploit what most IT specialists consider the weakest link in a company's security system: their employees. No company can be certain they won't be targeted by cyber thieves using a *Cyber Deception* scheme, and no company can be sure one of their employees won't fall victim to their scheme.

2014 Spear Phishing Attacks by Business Size[2]



Is My Company Covered for a Cyber Deception Attack?

Unless you have reviewed your current policies recently, the answer is probably not. Coverage for *Cyber Deception* is usually found in an endorsement to a Cyber/Privacy or Commercial Crime policy. These endorsements are new extensions of coverage that insurance companies have begun to offer in response to the escalating threat of *Cyber Deception*. If it is available, the coverage is often limited, and subject to additional underwriting and a sub-limit.

What Would a Cyber Deception Extension Cover?

In short, a *Cyber Deception* extension would indemnify you, up to the stated limits, for money and/or securities that were lost due to an act of *Cyber Deception* perpetuated against your firm. Some of these endorsements will also cover losses due to telecommunications fraud and wire transfer fraud. *Cyber Deception* endorsements are not standard, and will vary widely by company.

Why choose Axis Insurance Services?

Each insurance company has its own endorsements, restrictions and coverage extensions, so you need a qualified professional to help evaluate your options. Unlike most brokers, our professionals specialize in professional and management liability – including cyber/privacy and commercial crime, and are nationally recognized. Our years of expertise in the industry allow us direct access to high-quality insurance carriers, extremely competitive rates and the ability to customize a *Cyber Deception* extension specifically for your firm. Call us for a quick review of your current policy to ensure your business is properly protected.

[1]Hillard Heintze The Front Line Report
[2]Symantec Internet Security Threat Report, April 2015, Volume 20

11/1/15

Contact our experts today to find out how you can protect your business.

Axis Insurance Services, LLC
795 Franklin Avenue, Suite 210
Franklin Lakes, NJ 07417

www.axisins.com
P: 201-847-9175
F: 201-847-9174

Cyber Deception/Social Engineering

Claim Scenarios:

Manufacturing Company
An employee of an electronics manufacturer received phone and email instructions from an existing parts supplier. She was asked to wire payment of their open invoices to a new account the supplier had set up. After wiring over $500,000.00 to the vendor, the company learned that the email had not come from their parts supplier, but from a cyber thief. In this case, the thief used information right on the company's website to target the employee responsible for vendor invoice payments.

Real Estate Attorney
After conducting a closing and receiving the proceeds of the sale, a real estate attorney received an email from the seller's attorney to wire the proceeds to the seller's bank account. The attorney complied with the written instructions he received. It was only after receiving a telephone call from the seller's attorney that he realized that he had received a fraudulent email, and had wired over $125,000.00 to a cyber thief's account. Apparently, the cyber thief had been monitoring the attorney's email and knew he would be expecting wire transfer instructions.

Energy Company
An energy company's vice president received an email from his company's CFO instructing him to wire $2,000,000.00 to the bank account shown in the email. The email contained detailed instructions on how the payment was to be posted in their accounting system. It even included an attachment from the company's CEO, with a request to keep the pending acquisition of a competitor in the strictest confidence. The vice president then completed a wire transfer of over $2,000,000.00. It was only later, after the $2,000,000.00 was long gone, that the vice president learned that neither the CFO nor CEO had any knowledge of the email.

Technology Firm
A well-know public company based in Silicon Valley was targeted by cyber thieves through one of the company's Asian subsidiaries. Using a series of authentic looking emails, the cyber criminals were able trick employees in their finance department into disclosing account numbers, user names and passwords. They then used this information to transfer $47,000,000.00 from the firm's accounts into overseas bank accounts. Some of the money has been recovered, but as of September, 2015, $31,000,000.00 remains missing.

Insurance Agency
An insurance agency employee received an email from the agency's owner, followed by a series of frantic text messages instructing her to wire $43,800.00 in premium to an insurance company's account, before their client's policy was cancelled for non-payment. The client owned a hotel on Florida's South East coast, and she was concerned that if the policy cancelled, they might not be able to replace it. The employee was unable to reach the agency's owner by phone, but she wired the funds anyway, to keep the policy from cancelling. Later, when the agency's owner returned from an all-day seminar, she learned that the emails and text messages had been fraudulent. The cyber thieves had apparently monitored the agency's emails, and knew the owner would be unreachable by phone that day.

These are only claims examples: minor changes from actual suits have been made to protect the confidentiality of all clients.

[1]Hillard Heintze The Front Line Report
[2]Symantec Internet Security Threat Report, April 2015, Volume 20

11/1/15

Contact our experts today to find out how you can protect your business.

Axis Insurance Services, LLC
795 Franklin Avenue, Suite 210
Franklin Lakes, NJ 07417

www.axisins.com
P: 201-847-9175
F: 201-847-9174