Social Engineering Coverage: Is that on the Crime or Cyber Policy?

A frequently asked question from my school clients is, “Will my crime or cyber policy cover a social engineering attack that happens through the computer for fraud or funds transfer fraud?”

Let me start with defining Social Engineering Fraud (SEF).

This astonishingly effective fraud happens when unsuspecting employees, acting in good faith, comply with instructions sent via email to make a wire transfer or another type of transfer to a fraudulent third party replicating a legitimate correspondence.

Here at TRICOR, we’ve seen this before. Our client, a Chief Financial Officer, in the manufacturing industry received what he thought was an email from the President of the company that directed him to send an electronic funds transfer to a third party. But, the email was not from the President of the company but was, in fact, a fraudulent third party.

It is important to be careful reviewing a crime policy.

Wording can vary from carrier to carrier. I have attached an “ISO” endorsement following this article that can be added to your crime policy that will add the “fraudulent impersonation coverage.” Some people confuse fraudulent impersonation coverage with social engineering (cyber deception) covered within your cyber policy. ***This is why it’s important to read and understand your policy.***

Here are some key words to look for in your policy

1. **Voluntary Parting Exclusion:** The so-called voluntary parting exclusion is a key exclusion carriers may use in declining coverage on a crime policy. The exclusion may read, “no coverage for loss arising out of anyone on the Insured’s express or implied authority being induced by any dishonest act to voluntarily part with title to or possession of any property.” The key here is the wording “*being induced*” and “*voluntary act*” which are a definition of an SEF.
2. **Computer Fraud:** This generally covers a school for direct loss of money or property sustained by the school resulting from computer fraud committed by a third party.
    - Computer fraud is generally defined in crime policies as the unlawful taking of money resulting from a computer violation.
    - Computer violation is generally defined as an unauthorized entry into or deletion of data from a computer system committed by a third party.

Something to consider

Carriers may argue that this coverage hasn’t been triggered because the fraudulent payment instructions came via email, and email by its nature is an authorized entry and it needs to be unauthorized to trigger coverage.

3. **Funds Transfer Fraud:** Can generally be defined as fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions, other than forgery, purportedly issued to a financial institution, directing them to transfer, pay or deliver money from any account maintained by the organization, *without* such organization’s knowledge or consent.
    a. This generally covers organizations for direct loss of money sustained by the insured resulting from funds transfer fraud committed by a third party.

What you should know

A key reason for a claim denial is with funds transfer fraud, “funds are transferred *with* the organization’s knowledge or consent," which for SEF the organization did have knowledge and did consent. Even if it was on “mistaken belief” the coverage requires transfer without knowledge or consent.

Social Engineering on a Cyber Policy

Social engineering in cyberspace is an intrusion technique. Hackers use it to gain access into your system or trick your employees into violating security protocols in order to access sensitive data or make unauthorized money transfers.

How does this happen?

It usually involves employees acting in good faith, wire transferring money to fraudulent accounts they believe are legitimate. Criminals do this by:

1. Gaining information about the structure, key employees and executives of a target company through websites and social media accounts.
2. They typically then send a fraudulent email that’s constructed to resemble a legitimate email requesting a wire transfer.

As you can see, there can be confusion as to where the coverage may come from. A school should review its insurance to ensure proper coverage is in place to respond to a potential claim.

Remember, many insurance carriers offer a specific social engineering endorsement on the crime policy to cover this type of loss.

The bottom line

This type of loss could be covered either by a cyber or crime policy. Be careful of brokers and insurance consultants that do not understand this distinction. A good resource is www.eriskhub.com to complete a cyber audit of your school and for webinars on educating staff on cyber and crime risks.

Please contact us for help or questions with your insurance needs.

TRICOR INC. INSURANCE

John Gibson
Partner/Vice President TRICOR Insurance
jgibson@tricorinsurance.com
877-468-7426 x1714

POLICY NUMBER:

CRIME AND FIDELITY
CR 04 17 11 15

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

FRAUDULENT IMPERSONATION

This endorsement modifies insurance provided under the following:

COMMERCIAL CRIME COVERAGE FORM
COMMERCIAL CRIME POLICY
GOVERNMENT CRIME COVERAGE FORM
GOVERNMENT CRIME POLICY

SCHEDULE

Check the appropriate box(es):

I. Fraudulent Impersonation Of "Employees" Included: Yes ☐ No ☐

- ☐ **A.** Verification Is Required For All "Transfer Instructions"
- ☐ **B.** Verification Is Required For All "Transfer Instructions" In Excess Of **$**
- ☐ **C.** Verification Of "Transfer Instructions" Is Not Required

II. Fraudulent Impersonation Of "Customers" And "Vendors" Included: Yes ☐ No ☐

- ☐ **A.** Verification Is Required For All "Transfer Instructions"
- ☐ **B.** Verification Is Required For All "Transfer Instructions" In Excess Of **$**
- ☐ **C.** Verification Of "Transfer Instructions" Is Not Required

Information required to complete this Schedule, if not shown above, will be shown in the Declarations.

With regard to this Fraudulent Impersonation endorsement, the provisions of the Coverage Form or Policy to which this endorsement is attached apply, unless modified by this endorsement.

A. The following Insuring Agreement is added to Section **A. Insuring Agreements:**

Fraudulent Impersonation

1. "Employees" (if indicated in Section I. of the Schedule)

We will pay for loss resulting directly from your having, in good faith, transferred "money", "securities" or "other property" in reliance upon a "transfer instruction" purportedly issued by:

a. An "employee", or any of your partners, "members", "managers", officers, directors or trustees, or you (if you are a sole proprietorship) if coverage is written under the Commercial Crime Coverage Form or Commercial Crime Policy; or

b. An "employee", or any of your officials if coverage is written under the Government Crime Coverage Form or Government Crime Policy;

but which "transfer instruction" proves to have been fraudulently issued by an imposter without the knowledge or consent of the person in Paragraph **1.a.** or **1.b.**

2. "Customers" And "Vendors" (If indicated in Section II. of the Schedule)

We will pay for loss resulting directly from your having, in good faith, transferred "money", "securities" or "other property" in reliance upon a "transfer instruction" purportedly issued by your "customer" or "vendor", but which "transfer instruction" proves to have been fraudulently issued by an imposter without the knowledge or consent of the "customer" or "vendor".

3. Verification

a. The following is a precondition to coverage under this Insuring Agreement:

(1) If option **I.A.** and/or **II.A.** is selected in the Schedule, you shall verify all "transfer instructions"; or

(2) If option **I.B.** and/or **II.B.** is selected in the Schedule, you shall verify all "transfer instructions" in excess of the amount shown;

according to a pre-arranged callback or other established verification procedure before acting upon any such "transfer instruction".

b. If option **I.C.** and/or **II.C.** is selected in the Schedule, verification of "transfer instructions" is not a precondition to coverage under this insuring agreement.

B. Under Section **E. Conditions:**

The **Territory** Condition is replaced by the following:

Territory

We will cover loss that you sustain resulting directly from an "occurrence" taking place anywhere in the world.

C. The following definitions are added to Section **F. Definitions:**

1. "Customer" means an entity or individual to whom you sell goods or provide services under a written contract.

2. "Transfer instruction" means an instruction directing you to transfer "money", "securities" or "other property".

3. "Vendor" means an entity or individual from whom you purchase goods or receive services under a written contract.