Capitol Special Risks

Invoice Manipulation Coverage: The Coverage Insureds never knew they needed

Dorothea P. Westin, RPLU, CRM, CIC, CPIW
Written on August 26, 2019

The newest threat that is challenging corporate America is ***Invoice Manipulation***. Companies of all sizes are being targeted by Cyber "Bad Actors", commonly known as hackers and cyber thieves. **Invoice Manipulation** is happening at an alarming rate and many of the claims are not being covered because most insurance policies don't have a coverage trigger that applies to this type of claim.

So what is **Invoice Manipulation** and why is important? **Invoice Manipulation** is the flip side of ***Social Engineering*** scams. In a **Social Engineering** scam, the Insured's company or more specifically an employee of the company is tricked via a hack or phishing scam to voluntarily part with money, products, services or goods. **Invoice Manipulation** is more devious in nature. It happens when the customers or vendors of an Insured are tricked by a Bad Actor using legitimate email and data of the Insured to get the customer or vendor to alter a payment or deliver of products, services or goods to the wrong location that is controlled by the Bad Actor. Generally, the way this happens is a Bad Actor either gains access to one of your employee's emails by a successful phishing scam or by breaching their personal accounts and securing a password they use at work. The scariest part of **Invoice Manipulation** is that it takes time. The Bad Actor sits and waits watching your system, learning your habits, seeing all of that employee's correspondence, and specifically learning how your company and its customer or vendors work together. Then they wait until the right time to ask your customer or vendor to change a payment via wire to a new bank, or have standing deliveries redirected to a new worksite using the compromised account and then deleting the request and correspondence before your employee sees it. The terrifying repercussion is that the Insured has no idea the events have transpired until they go to either follow up for payment or secure more supplies, at which point they learn their money or order is gone and there is nothing they can do.

The unfortunate misperception is that Insureds think this type of incident is already covered in their policy. Many people believe since it starts with a phishing or a hack attack that their policies will have coverage under the **Social Engineering** clause. Again, since the **Social Engineering** clause is only designed to cover an instance when their own employee is being socially engineered or manipulated to give up money, products, services or goods, there is no coverage. **Invoice Manipulation** is not about your employee giving up money, products, services or goods. It's about someone portraying themselves as your employee

and convincing your customers and/or vendors to redirect payment, products, services or goods. This action, while similar in nature, is not the same. The crime is perpetrated on another party outside of your firm. So, it should be their problem right? It doesn't quite work that way because the customer or vendor has an email or communication that legitimately came from your company and is related to actual payment, products, services or goods intended to be from you. The truth is, if your server sends the request, your customer or vendor is not responsible for your loss. While this seems unfair, the reality is that the courts and the insurers have defined the distinction between the two coverages.

Insureds or the victims often argue and believe they have not done anything wrong so the transaction is void and should not be counted against them. Their logic is often that it is the customer's or vendor's **Social Engineering** issue and not their problem. Unfortunately, upon forensic review, the Insured often finds they were hacked or phished. Learning that Cyber **Social Engineering** does not cover the loss, many try to look to other coverages. The next path would be Crime Coverage. Unfortunately, unendorsed Crime policies are only designed to cover Crime committed by your employees or theft at the business location of the Insured so neither of these coverage triggers apply. Since neither the unendorsed Cyber policy nor the Crime policy are triggered by this action, the customer or vendor deems the matter closed and the problem truly becomes that of the Insured who was actually infiltrated by a Bad Actor in the first place.

This brings us back to the needs of an Insured who has either not been paid or does not have the goods/services they need to conduct their business. How do they get coverage? As we have reviewed, it is not a **Social Engineering** coverage issue. **Invoice Manipulation** coverage is currently the clearest insurance clause that can respond to these types of claims. There are specific terms and conditions surrounding **Invoice Manipulation** claims. All Cyber policies are non-standard so there is not one magic definition. Below I have referenced the Beazley Breach Response Endorsement CB-133-001 as it gives a separate Insuring Agreement, limit, retention and definition. Please see the Insuring Agreement and Definitions that create the coverage.

> **INSURING AGREEMENTS** is amended to include:
>
> **Invoice Manipulation**
>
> To indemnify the **Insured Organization** for **Direct Net Loss** resulting directly from the **Insured Organization's** inability to collect **Payment** for any of the following goods, products or services after such goods, products or services have been transferred to a third party, as a result of **Invoice Manipulation** that the **Insured**

first discovers during the **Policy Period:**

<Precise Description of Goods/Products/Services>

DEFINITIONS is amended to include:

Direct Net Loss means the direct net cost to the **Insured Organization** to provide goods, products or services to a third party. **Direct Net Loss** will not include any profit to the **Insured Organization** as a result of providing such goods, products or services.

Invoice Manipulation means the release or distribution of any fraudulent invoice or fraudulent payment instruction to a third party as a direct result of a **Security Breach** or a **Data Breach**.

Payment means currency, coins or bank notes in current use and having a face value.

Since this is a non-standard coverage which must be linked back to key definitions within the Cyber policy, each carrier's endorsement will be uniquely different from each other. The review of **Invoice Manipulation** as defined in this endorsement does include payment and goods, products or services is coverage that can reimburse an Insured who had a third party Bad Actor impersonate the Insured using the Insured's credentials to steal the payment or goods/services originally intended for the insured.

As with all non-standard products, the buyer must be aware of what they are purchasing. Not all insurance companies are offering the coverage. The Insurers who do offer Invoice Manipulation coverage also have varying terms, conditions and limits which may apply. The safest way to make sure you are getting Invoice Manipulation coverage is to ask for it and review the terms, conditions, limits and retentions, some forms may even have co-insurance options. As the coverage evolves it will become more standard but right now the forms vary from one another.

The final analysis - cyber criminals are getting smarter and cyber insurers are working hard to keep up with the demand to protect consumers. If you bought your cyber policy before late 2018, have your agent review it to make sure **Invoice Manipulation** coverage was added by endorsement.