PARKER | SMITH | FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

PRACTICE GROUP:
PROFESSIONAL SERVICES

MAY 21, 2019

PROTECTING ORGANIZATIONS AGAINST INVOICE MANIPULATION

Gregor Hodgson | Principal, Vice President

Finance teams in most professional service organizations are by now quite accustomed to receiving phishing emails that purport to be from an officer of the company requesting the recipient to immediately wire funds for a new project or piece of equipment. Most people now know to call the customer or vendor in question when they receive an email telling them that the customer has changed banking accounts. Service organizations should now have controls in place to make sure that an unwitting employee can't simply wire funds without verifying that the destination is the correct location for those funds. As a professional services organization, your company has probably done the same. But, what about your customers and vendors, have they set up similar controls? Could your organization be liable if your customers or vendors are tricked by a social engineering scheme? The answer may surprise you.

> Could your organization be liable if your customers or vendors are tricked by a social engineering scheme?

PHISHING YOUR CUSTOMERS - SCENARIO

Consider the following example: A crook hacks into your email system and takes over a billing clerk's email account. The hacker then sends emails to your customers requesting they send payments, not to your account, but to a new bank account that the hacker controls. When a historically reliable customer's account become past due, you send follow up statements. However, the hacker has programmed new rules into your email system, such that the past due statements are redirected back to the hacker and your customer never receives the late notices. By the time you and the customer discover the issue, several payments have gone to the wrong bank account and none of the payments can be traced.

After a thorough investigation, you and your customer discover what has happened. Your customer is terribly sorry, but they inform you that they sent payment to the bank account to which they were directed by your computer system. They acknowledge that they failed to confirm the bank account change, but claim that they are not responsible for the loss as they have made payment as directed.

continued >

SOCIAL ENGINEERING COVERAGE PITFALLS

When you turn to your cyber insurance policy, you will discover that many crime and/or cyber policies have coverage for social engineering losses. However, this type of coverage applies to your employees being deceived and sending your funds to an unknown party. In the scenario above, you never had possession of any of the funds. Coverage for this type of loss is still not included in most cyber or crime policies. A few insurers have developed endorsements that provide a small amount of coverage for what is now being referred to as push payment fraud or invoice manipulation coverage. Consult with an experienced broker to discover if you have this type of coverage and whether any sub-limits of liability or other limitations apply.

In addition to securing insurance coverage, professional service firms should consider additional financial controls when utilizing wire fund transfers. The above scenario could have been avoided had the customer called and verified the change in banking procedures. If you allow customers to pay their bills using wire transfers, consider establishing agreements that outline which accounts they can wire funds into, as well as some controls that need to be observed before changes can be made to the designated accounts.

By mutually agreeing to utilize callback or other forms of dual authentication, both parties can better protect themselves when utilizing wire transfers for payment. In the above example, had an agreement been in place, the organization sending the bills may have been able to push back against their customer for not using some form of dual authentication before changing the location of the deposit account. Talk to your bankers and accounts about what types of controls other professional services firms are using and talk to your insurance broker about payment fraud options under your cyber insurance policy.