O'HAGAN MEYER

RAPID RESPONSE & INCIDENT MANAGEMENT

Best Practices for Preventing & Responding to Cyber Theft & Wire Fraud

Cyber theft and wire fraud are common attacks that can have a devastating impact on your business. These attacks generally occur because of a business e-mail compromise or other computer network compromise. There are several simple steps you can take to prevent these types of attacks, and to respond in a manner that can minimize their impact.

Employee Training: In most cases, employees have an opportunity to stop cyber theft before money goes out the door. Training your employees to identify phishing scams, social engineering threats and indicators of e-mail compromise, will allow your employees to identify cyber theft attempts before any funds are transferred. Specific examples should be provided to your employees, since most cyber theft events follow a familiar pattern.

Policies and Procedures: Implementing appropriate policies and procedures is the most important step in fighting cyber theft and wire fraud loss. Specifically, your employees should be required to verify electronic payment instructions with the intended **recipient** of the funds, using a publicly available phone number, or a phone number that was previously verified, prior to authorizing an electronic payment. Verification should be performed each time a payment is made, but especially when new or changed payment instructions are involved. The verification should be documented, and appropriate sanctions should be in place for employees that do not follow the required policies and procedures.

Warn your Customers and Vendors: Provide information in writing to your customers and vendors regarding the risks of cyber theft and wire fraud. Advise your customers and vendors that you will never provide new or changed payment instructions via e-mail and require that they contact you via telephone prior to sending any electronic payment. Provide additional information to customers and vendors about typical cyber theft scams in your industry.

Contact your Bank: Immediately upon discovery of a misdirected electronic payment, you should contact your bank to notify them of the potential fraud. You should ensure that your bank contacts the receiving bank so that the receiving bank can freeze the funds in the receiving account. The sooner your bank is informed of fraud and takes action to recover the funds, the greater chance of minimizing the financial loss.

Contact your Insurance Carrier: After you have notified your bank, you should contact your insurance carrier. You need to notify your insurance carrier to ensure that all applicable notice requirements under your policy are met. Your insurance carrier will be able to assist with funds recovery and will determine whether additional assistance is required. Oftentimes, cyber theft is the result of an e-mail compromise, or computer system compromise, and a forensic investigation may be necessary to determine the extent of the compromise and to ensure that your e-mail environment and/or computer system are secure moving forward. This investigation can also determine whether any additional financial transactions are in jeopardy, or if there has been a data breach. If there has been a data breach, you may need to hire privacy counsel and provide data breach notification letters. Your insurance carrier can assist you in determining which services are recommended, along with which services are covered under your policy.

Contact Law Enforcement: You should contact all applicable law enforcement agencies to report any instance of cyber theft. Specifically, you should contact the FBI via their Internet Crime Complaint Center (www.ic3.gov) and should also notify the Secret Service's Financial and Cyber Crime Investigations Unit. If privacy counsel is retained by you, or assigned by your insurance carrier, they can assist in filing these reports. The FBI and Secret Service can be useful resources in investigating the incident and recovering the funds.

O'HAGAN MEYER

ATTORNEYS ▲ ADVISORS