Victor O. Schinnerer & Company, Inc.

CYBER EXTORTION

Extortion threats can come from anywhere

Cyber extortion occurs when a company receives threats to damage or shut down a company's website, e-mail server, or computer system or threatens to expose electronic data or information belonging to the company unless the company pays the criminal a specific ransom amount. Companies can be vulnerable to cyber extortion no matter where they are located, and whether the perpetrator is operating in the U.S. or halfway across the world. Companies who hold trade secrets or confidential information, or who are reliant on access to their computer systems to maintain operations can be particularly vulnerable.

CLAIM EXAMPLE

Smith & Smith, LLP, a midsize law firm, held confidential information on many of their clients, as well as information on merger opportunities they were exploring. A hacker based in Russia gained access to their computer system and the confidential information on it. The hacker then sent an email with a copy of a merger plan scenario and files on one of the firm's clients and threatened that unless they were wired $250,000 they would not only shut down the firm's computer systems, they would also publish all the data they obtained from the system.

HOW DOES THE SCHINNERER POLICY RESPOND?

Cyber Extortion coverage is included in the Schinnerer Cyber Protection Package standard form.

If Smith & Smith, LLP paid the hacker $250,000, the Cyber Extortion coverage would reimburse the firm and cover any fees accumulated from the Breach Response Team including legal and investigation services.

For more information, contact a Cyber Protection Package underwriter at vos.cyber@schinnerer.com.

Victor O. Schinnerer & Co., Inc. | Two Wisconsin Circle | Chevy Chase, MD 20815
Phone: 301-961-9800 | Fax: 301-951-5444 | www.Schinnerer.com | vos.info@Schinnerer.com