Victor O. Schinnerer & Company, Inc.

TAKE CYBER LIABILITY EXPOSURES SERIOUSLY

MANAGEMENT ADVISORY

Professional service firms are facing an increased exposure to cyber liability. Many firms do not take the necessary steps to secure their systems, guard their digital assets, protect confidential client information, and maintain productivity. Each firm should have digital protection protocols that help avoid or minimize data breaches as well as a plan to manage any breach that might occur. And that plan should include insurance coverage should firm operations be compromised.

COMMON SOURCES OF CYBER LIABILITY

Cyber liability problems that have disrupted firm operations often are based on one of three vectors:

1. insiders who are dissatisfied or recognize their ability to tap firm assets and use that access for harm or personal profit;
2. past employees who either take digital assets with them or to enact revenge against their former employers corrupt firm systems and information; and
3. hackers who know that confidential project data is vulnerable and hold digital information hostage until a ransom is paid.

Most firms allow unsafe digital behavior or have little in the way of protection protocols. Many firms lack appropriate limits on employees' access to confidential and sensitive information such as intellectual property, digital design data, and private information about clients, employees, and business partners. Some employees are allowed to load confidential documents onto their unsecured personal computers, smart phones, and the public cloud. A combination of employee knowledge of a firm's system and a failure to monitor insider behavior leads to some of the most damaging data breaches.

A disgruntled former employee who decides to steal or compromise the firm's digital assets before leaving can be a significant risk. Deleting important files, sharing proprietary or confidential client information with unauthorized third parties, remotely modifying or deleting critical design data, and tampering with the integrity of design documents can result from unauthorized access. Some former employees may use past access to company bank accounts and payroll systems and employees' personally-identifiable information to harm the firm and its employees.

HACKERS CAN WREAK HAVOC ON A FIRM

Although internal threats cause many cyber liability breaches, a malicious outsider is one of the greatest fears of professional services firms. A hacker could cause data inaccessibility through alteration or destruction. A firm would lose intellectual property and no longer be able to meet contract objectives and deadlines. Attackers who gain access to a firm's data can encrypt it using ransom-ware and extort payment to regain access to information. Firms that do not properly preserve digital assets through robust back-up systems often have no alternative but to pay the ransom.

Construction projects today are increasingly dependent on digital technology. The adoption of BIM and the increasing use of digital technologies in designing, constructing, and operating buildings and infrastructure are transforming the way the industry works. The concept of collaborative work through the sharing and use of detailed models and large amounts of digital information requires that parties be aware of vulnerability issues and take appropriate control measures. Improper access controls could lead to an attack severely disrupting progress on a project, causing delays or remedial work that could lead to significant claims from owners, lenders, or other stakeholders. And if confidential information on the structure or systems of projects is accessed by unauthorized parties, the safety of the owners and users of the buildings or infrastructure could be put at risk.

A DIGITAL SECURITY STRATEGY IS CRITICAL

Creating a strategy for improving digital security can be challenging. In addition to appropriate firm practices—such as requiring secure password naming conventions and limiting Internet access to many records—educating employees on the dangers of digital data security and the need to follow proper procedures is critical. If network integrity is compromised, sophisticated malware can create liability issues by using a firm's network to compromise and infect other networks that may be integrated on a continuing or project basis.

Cyber losses involve more than payouts to third parties injured by the wrongful disclosure of confidential information. Firms are subject not only to providing legally required notices and meeting other regulatory obligations, but may face breach of contract, confidentiality, and other legal challenges. In addition, firms must also pay for up-front investigation costs, data restoration and business interruption costs, and public relations costs. A significant data breach can lead to millions of dollars in costs and productivity losses. So firms need to protect their operations and insure their cyber risks with a policy appropriate for their industry and operations.

Visit **www.Schinnerer.com/AEriskmanagement** for more information or contact us at **vos.RMeducation@Schinnerer.com**.

For more information on practice management, please visit our website at **www.Schinnerer.com/AEriskmanagement**, or you can reach our Risk Management Department at 301-961-9878, fax at 301-951-5496, or email at **vos.RMeducation@Schinnerer.com**.

Victor O. Schinnerer & Company, Inc.
Two Wisconsin Circle
Chevy Chase, Maryland 20815