Cyber Risk: Keeping Client Information Safe

By: Andrew J. Fotopulos & David R. Jacavone

An issue that has been making headlines in the financial services sector lately is the growing threat of cyber security. Security breaches present a vast range of severity with regards to the type of confidential information that has been compromised. More often than not, this all seems to lead back to one concern, the structural integrity of the infiltrated firm. Clients might ask themselves "Was the firm or advisor not keeping my information safe enough or was the hacker's strategy just too far advanced for current security measures to catch it?" Whichever the case, clients are feeling less confident.

We often educate our clients about the value of Directors & Officers (D&O) Liability. Did you realize that there may be coverage under D&O for client and regulatory claims? A board member's alleged breach of fiduciary duty, or lack of due diligence to secure client's information could trigger coverage. Are you completing due diligence on those third-party providers that have access to client and employee personal information? What internal controls do you have in place to avoid access sensitive client data?

Latest industry statistics show that while large corporations and banks make the headlines when attacks happen, 36% of all targeted attacks were on businesses that have 250 employees or less. So this isn't just a Fortune 500 issue. Accidental misuse of data by employees is also a root cause of these breaches. In fact, it is the number one risk of data loss. In 2013, Forrester research found that 36% of breaches stemmed from inadvertent misuse of data by employees. This is caused by:

- opening infected email attachments
- unattended/unlocked computers
- poor security passwords
- unsecured mobile devices that have confidential information stored on them

Clearly big and small firms alike should have cyber liability policies in place to protect the firm if and when infiltration occurs. Your incumbent insurance broker should be able to coordinate your Errors & Omissions policy to include D&O. Nonetheless, you still need to be cautious of exclusions that may exist eliminating coverage under the D&O portion of your policy. Exclusions for mechanical breakdown and privacy violation along with others may eliminate the availability of coverage.

While it is more difficult to carve out Cyber Coverage under your D&O policy, there are stand-alone policies that cover far beyond what would be picked-up under the traditional D&O policy while including coverage for claims arising out of the lack of care and due diligence. Some of the additional coverages may include

- privacy and network security liability
- first and third-party liability
- wrongful disclosure of data
- wrongful disclosure of HIPAA-protected health information
- breach of security, fines and penalties, identification theft, credit monitoring, forensic testing, e-mail fraud fund transfer, notification cost, etc.

When trying to transfer this risk to the fullest extent possible, be sure you are working with an insurance provider who understands your business and the unique exposures faced by those in the investment community. While there may be a lot of questions about what is covered, Starkweather & Shepley's Investment Industry Practice Group has the answers.

**Andrew J. Fotopulos and David R. Jacavone are part of the Investment Industry Practice Group of Starkweather & Shepley Insurance Brokerage, Inc.*