GUEST COLUMN

A Primer on the Difference Between Cyber and Financial Institution Fidelity Bond Insurance Policies

By Mike Oppe, Senior Vice President, Financial Institutions, Chubb Insurance*

The annual Investment Management Compliance Testing Survey results for each of the last six years (2014-2019) rank cybersecurity as the "hottest compliance topic" scored by respondents. (The survey is conducted by the Investment Adviser Association (IAA) and ACA Compliance Group.)

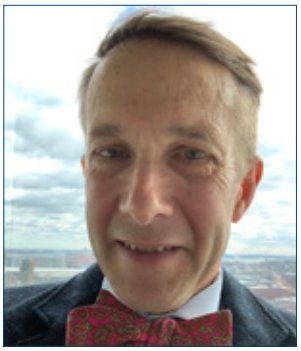
It is noted that the IAA survey rankings of cybersecurity as the "hottest compliance topic" strongly correlate with the heightened adviser awareness and SEC regulatory focus over a similar time period. In fact, the SEC created a new Cyber Unit within Enforcement and has targeted cybersecurity as an examination priority each consecutive year since 2017.

In addition to increased controls and practices like mock exams instituted by advisers, the 2019 IAA Compliance Testing Survey also points to an increasing uptake in the purchase rate of cyber insurance policies, increasing from 33 percent in 2016 to 66 percent in 2019.

Notwithstanding this increasing cyber standalone policy purchasing rate, we continue to observe a significant amount of confusion regarding the perils covered by cyber policies versus other policies, particularly the fidelity bond.

A key step to sorting out the confusion is understanding what type of perils are covered and where, with a goal of achieving a more comprehensive insurance risk transfer solution.

With the rise in IAA annual survey respondent confirmations of having had a "cybersecurity incident" reaching 39 percent in 2019 as compared to 18 percent in 2016, getting the answer to the question of "Do I have the right coverage?" is an increasingly important consideration.



Mike Oppe, Chubb Insurance

"The coverage afforded by a standalone cybersecurity liability policy and a fidelity bond are complimentary and together provide a comprehensive risk transfer solution to cybersecurity related exposures."

Difference with a Distinction

A cyber insurance policy for investment advisers and other financial institutions typically provides both first party coverage and third party liability coverage, including coverage for incidents arising out of the unauthorized access to or use of a computer system (*e.g.,* a hack) resulting in the *loss of non-public Personally Identifiable Information or confidential client data*. For example, first party cyber coverage may cover costs to remediate a data breach where client information has been compromised, such as notification expenses and credit monitoring. Third party liability coverage may cover damages and defense costs incurred by the organization arising from an action in connection with such a data breach or failure of the organization's network security.

By comparison, a fidelity bond is a first party policy, which intends to cover the *direct loss of client and adviser capital due to dishonest acts by employees,* as well as the unauthorized access to, or entry of malicious software into a computer system (*e.g.,* a hack). For example, fidelity bond coverage might include the loss of client capital due to their account being fraudulently accessed by a hacker, for which the Insured (the adviser) reimburses its client.

Coverage afforded under the fidelity bond for loss as a result of a computer system compromise continues to evolve within the industry. Rapid advances in technology used by advisers to manage client assets (*e.g.,* cloud hosting and mobile applications) are driving the development of new coverage extensions to address some of these emerging exposures.

In particular, loss of client and adviser capital resulting from social engineering fraud (*e.g.,* phishing, baiting, fake president fraud, or email compromise) continue to increase, giving rise to the need for specialized coverage to address this risk. Such specialized coverage may need to be endorsed onto a standard fidelity bond.

Continued on page 22

Continued from page 21

Focus – Social Engineering Fraud

According to the FBI, social engineering fraud cost businesses in the United States approximately $1.6 billion from June 2016 to May 2018.

Hackers are using increasingly sophisticated methods to disguise themselves as legitimate parties, defraud advisers, and avert internal controls.

Through trick and artifice, fraudsters seek to capitalize on well-intentioned employees to defeat strong internal controls and training, resulting in employees unknowingly transferring funds to them.

Internal controls such as multifactor authentication and dual signature thresholds have shown to be helpful deterrents to losses. These tools and procedures tend to slow down the quick response timing of social engineering-type funds transfer requests and bring a greater level of transparency into the transaction.

Several recent high-profile lawsuits have resulted in certain courts finding some coverage for social engineering loss under the standard base fidelity bond. In response to this development, many carriers have added new exclusionary language to close this door to

coverage and are cautiously adding back coverage for social engineering losses on an account-by-account basis for qualifying risks via a special endorsement.

Carefully reviewing the fidelity bond with your qualified insurance agent or broker is suggested to ensure familiarity and understanding of the coverage afforded under the bond and to avoid the ill-timed discovery of a possible gap in coverage after a loss.

Conclusion

Investment advisers are facing ever increasing reputational exposure and regulatory scrutiny as a result of their fiduciary responsibility to safeguard client capital in this digital era.

Loss as a result of social engineering of employees and fraudulent impersonation of clients is increasing at an alarming rate.

The coverage afforded by a standalone cybersecurity liability policy and a fidelity bond are complimentary and together provide a comprehensive risk transfer solution to cybersecurity related exposures.

**Mike Oppe is Senior Vice President of Chubb's Financial Lines. He can be reached at moppe@chubb.com.*

The opinions and positions expressed in this document are the author's own and not necessarily those of Chubb. The information provided is not intended to provide any legal or other expert advice as to any of the subjects mentioned, but rather is for general information only. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Actual terms and conditions of coverage may vary. This document is solely for informational purposes.