Examples of how your peers are seeking to strengthen their vendor contracts

Published on: 3/28/2019 Content area: Investment Adviser Comments?

The latest twist in OCIE's ongoing interest in how you're protecting your firm's cybersecurity plunges into how deeply you're scrutinizing your vendors' cyber protections.

Ben Anderson, principal with **Anderson PLC** in Minneapolis, reports examiner interest stretching from Boston to San Francisco probing how advisers are measuring their vendors' cybersecurity. "The focus is on material vendors," he says, meaning those that have access to your sensitive data.

Once again, cybersecurity appears among OCIE's 2019 exam priorities. This will probably be an annual occurrence as long as cyber bad guys ply their sinister trade on the Internet (**IA Watch**, Jan. 2, 2019).

IA Watch asked CCOs recently how they're revising their vendor contracts – when they have the power to do so – and most noted they're focusing on cybersecurity (**IA Watch**, March 31, 2014).

Sailingstone Capital Partners ($4.6B in AUM) in San Francisco hired outside counsel to review three vendor contracts and to suggest changes. "We chose our three highest dollar contracts," says CCO **Kathlyne Kiaie**.

A data security addendum

The exercise resulted in a data security addendum. "It can be appended to any standard vendor contract to ensure that you are protected on the info-tech front," says Kiaie. The addendum deals with industry standards; data safeguards; security audits; required notification of a cyber incident within 24 hours; connecting to the adviser's network; EU data protections and more.

Clark Capital Management Group ($7.2B in AUM) in Philadelphia has sought to harden provisions limiting the firm's liability and indemnification to decrease the firm's cybersecurity risks, says CCO **Conor Mullan**.

Congress Wealth Management ($1.6B in AUM) in Boston updated cybersecurity clauses to match Massachusetts' legal definitions of personally identifiable information. CCO **Candace Cavalier** also pushed a clause requiring the vendor to notify the firm of a breach and insisting that the vendor acquire cybersecurity insurance.

It's natural to seek these types of provisions only with vendors that have access to your sensitive data. "It depends upon the services that they're providing," says **Joseph McDermott**, CCO at **THL Credit Senior Loan Strategies** ($3.7B in AUM) in Chicago. So language that binds a vendor to protect the firm's data won't make its way into a contract with the adviser's pricing vendor, notes McDermott.

Lacking clout

Many advisers can't insist upon contract clauses. "We're too small to effect any change in a contract," says **Jillian Carlson**, CCO at **ICW Investment Advisors** ($146M in AUM) in Scottsdale, Ariz.

ICW has contracted with a vendor to help check on its other vendors. The RIA has hired **Vendor Insight** to do due diligence on its vendors. "It is extremely expensive," notes Carlson. The cost is about $1,200 per vendor. For that price, the RIA gets a vendor's SOC1 report, a confirmation the vendor has insurance, and a peek at the vendor's cybersecurity, BCP and privacy policies, she adds. Vendor Insight produces a report on each vendor ICW asks about.

Vendor Insight also will look into the cybersecurity of 4th parties, that is the vendor's vendors, noted Carlson.

Who owns your data?

Don't forget who owns the data in your vendor contracts, states **Peter Mafteiu** with **Sound Compliance Services** in Gig Harbor, Wash. Your contracts should detail what happens to your data should you change vendors. This is important because the **SEC** could consider the data a required book and record that you should have access to,

he adds (**IA Watch**, July 9, 2012).

Another important provision sets out when the vendor would have to notify you of a data breach. It's reasonable to give a vendor some time to assess a potential breach, says attorney, author and former RIA CCO **Tery O'Malley**. He believes one week is a fair deadline for a vendor to report a breach.

He also recommends another clause that's unrelated to cybersecurity. This would be a non-disclosure provision. Say, an adviser obtains certain information under an NDA. This clause would allow the adviser to share that information without notifying the other party should the topic come up in a routine SEC exam. "If you don't ask for that carve out, you could find yourself in a situation where" you have to notify parties of a routine exam, O'Malley notes.

11 provisions to consider

There are many other clauses you may consider for your contracts. One source recommends 11 key provisions: 1. A relationship clause (defining how the two parties will work together); 2. Contract term and termination; 3. Services (what are you getting?); 4. Payment; 5. Insurance; 6. Indemnification; 7. Protection of confidential data or non-disclosure; 8. Intellectual property (data ownership); 9. Compliance with laws; 10. Governing law and jurisdiction; and 11. Arbitration.

Mafteiu has seen advisers insist on a non-compete clause. This would prevent a consultant from revealing to third parties an adviser's investment strategy.

Carlson notes she has been working with her custodian **Fidelity** for more than a year trying to get the firm to change a liability provision in its contract. Fidelity insists the adviser assume the liability when using a third-party vendor, even one that Fidelity recommended and that uses the custodian's data feed. She reports progress on the negotiations but no resolution yet.

Anderson shares a vendor contracting checklist he has created. He saves a more formal version for his clients but this checklist can be a good starting point for you. It would list provisions (e.g., description of products, fees, most favored nations clause, etc.) and what would be necessary for each (e.g., representation, warranty, covenant or negative covenant).

Take cybersecurity again. You may wish for the vendor to warrant that it uses "some type of commercially reasonable test," like a penetration test, to detect cyber weaknesses. Next, a covenant would have the vendor pledging to maintain recognized cybersecurity standards to detect and deter intrusions and to notify you of breaches, says Anderson.

If you happen to have enough clout, you next may mandate real-time reporting of cyber test results and even the right to visit the vendor's offices to assess its cybersecurity program in-person, he adds.

undefined undefined/Vendor Contracts/Getty Images Plus

Indexed by: Compliance Best Practices | Cybersecurity |

Back to Search Results /