

[Blogs](#)

May 15, 2015

Transfer and Sub-Transfer Agent Cybersecurity: Implementing SEC Guidance

The cybersecurity threats faced by mutual fund transfer agents (TAs) and sub-transfer agents (Sub-TAs) are unique because their information technology (IT) networks house a massive amount of personally identifiable information (PII) belonging to the funds they serve (Fund PII).^{*} In its recent [IM Guidance Update on Cybersecurity](#), the SEC staff stressed boards' responsibility to oversee the management of "cybersecurity threats and vulnerabilities so as to better prioritize and mitigate cybersecurity risk." Fund boards can work to meet the staff's expectations in this regard, and protect the privacy of Fund PII, by incorporating regular evaluations of TA and Sub-TA cybersecurity practices into their overall risk oversight. "Because funds and advisers rely on a number of service providers in carrying out their operations," the staff explained in its cybersecurity guidance, it might also be appropriate to "consider assessing whether protective cybersecurity measures are in place at relevant service providers." In the context of TA and Sub-TA operations, such due diligence should generally focus on: **Data Flow and Access**. Boards should consider working with their funds' adviser to map the flow of fund data, including PII, to the TA any Sub-TA. Once this mapping is complete, boards can assess the risks associated with various data recipients. During the mapping stage, boards should seek to:

- understand how and why each party uses the data it receives;
- ascertain the level of cybersecurity risk associated with each party's IT systems, including the potential for third party Sub-TA networks to infect the TA's IT infrastructure; and
- identify the risk mitigation procedures in place for all exceptions to the TA's generally applicable security standards.

Boards should also consider devoting substantial attention to the access controls that TAs and Sub-TAs have in place for their employees and other network users. As the SEC staff explained in the cybersecurity guidance, strategies should be in place that are designed to control access to systems and data "via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation, and system hardening." **IT/Data Security Compliance**. The SEC staff has affirmatively stated that fund service providers should have in place "written policies and procedures...that monitor compliance with cybersecurity policies and procedures." Accordingly, all recipients of Fund PII and other fund data should have in place industry-standard, written network and IT/data security programs designed to protect that information. Industry standards applicable to TAs and Sub-TAs include, but may not be limited to, those espoused in the ICI's FICCA framework. Cyber breaches of Fund PII through TA and Sub-TA networks may result in violations of federal law including, for example, federal Regulations S-P and S-ID and the federal anti-money laundering laws. State law is also especially important with respect to TA and Sub-TA operations, as many states impose strictly liability and costly fines for failure to immediately notify persons whose [PII is compromised](#). Boards should seek to ensure that policies and procedures, and/or contractual obligations, are in place to require that TAs and Sub-TAs provide immediate notice of any unauthorized access to Fund PII as well as any actual, probable or reasonably suspected breach of their networks. **Independent Control and Risk Assessments**. Boards should consider whether it is appropriate to require their TAs and Sub-TAs to provide periodic independent control/risk analyses. Auditors can conduct testing and provide boards with cybersecurity controls reports, including SSAE16s and related SOC1s, SOC2s, or SOC3s. In determining whether to require such reporting, boards should seek to understand how frequently TAs and Sub-TAs undergo independent IT/data audits and what the results of the most recent tests are. **Existing Contractual Liability/Indemnification Provisions; Cybersecurity Insurance**. Boards should consider working with counsel to understand what, if any, provisions in their funds' TA agreement, and in the TA's contract(s) with any Sub-TA(s), address IT/data security issues. In doing so, boards should consider, among all other questions they deem relevant, whether:

- the funds and their trustees and officers are indemnified against liabilities arising from unauthorized access to Fund PII and other data through TA and/or Sub-TA networks;
- insurance coverage exists to protect the funds and their TA and any Sub-TA from the costs of a cybersecurity breach; and
- it is appropriate to insist that the funds be added as third-party beneficiaries of any existing or future insurance policies held by the TA or any Sub-TAs and/or contractual indemnification that exists between the TA and a Sub-TA.

**Financial intermediaries that provide shareholder services to their customers (FI Customers) typically do not store or have access to the extensive Fund PII maintained by fund TAs and Sub-TAs. Generally speaking, funds are not liable for the PII belonging to FI Customers.*

Explore more in

[Investment Management](#)