By Thomas D. Giachetti

How to Bolster Cybersecurity During a Pandemic

The SEC is expecting advisors to be even more strident protecting client records in these times.

Since it first announced its "Cybersecurity Initiative" in April 2014, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations has been relentlessly setting its sights on RIA's information security programs. In fact, as recently as its 2020 Examination Priorities, OCIE noted it will "continue to prioritize information security in each of its five examination programs."

I spoke with our cyber expert, Cary Kvitka, regarding this increasingly important issue. Our firm has been helping RIAs draft customized cybersecurity policies and procedures under Regulation S-P, Rule 30(a) since April 2014.

Among other things, the rule broadly requires RIAs to adopt written policies and procedures addressing technical safeguards to protect their clients' data "against any anticipated threats or hazards to the security or integrity of customer records and information; and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

Therefore, when we customize written cybersecurity policies and procedures for our clients, we have turned to OCIE's published guidance to help identify and address their expectations.

PRACTICAL LESSONS

We've also learned practical lessons, one of which is that size really doesn't matter much to the SEC's examination staff. They seem to apply the same standards to RIAs of all sized firms, ostensibly because they all face the same type of palpable risks.

It is simply not enough for RIAs to adopt and enforce narrowly tailored policies and procedures for the protection of their clients' data from internal or external breaches. Rather, these policies must be evaluated and updated in response to operational changes and evolving risks.

As this pandemic clearly has changed the we conduct business and resulted in increased cybersecurity risks, this is an excellent time for RIAs to conduct a formal risk assessment and consider some changes to their policies, procedures, or infrastructure if appropriate. In doing so, OCIE's Cybersecurity and Resiliency Observations released not long before the pandemic took hold serves as a benchmark for industry best practices.

In this respect, SEC Chairman Jay Clayton himself opined, "Data systems are critical to the functioning of our markets and cybersecurity and resiliency are at the core of OCIE's inspection efforts."

Here are a few items we suggest RIAs specifically consider during those risk assessments, based OCIE's Cybersecurity and Resiliency Observations:

Access Management: OCIE highlights multi-factor authentication as an effective tool to mitigate both internal and external penetrations. In the context of the pandemic, RIAs should consider whether to implement or increase their use of multi-factor authentication, especially where users will be logging into firm systems from outside the firm's physical office.

Vulnerability Scanning: RIAs should establish a vulnerability management program that could scan network components, information systems, and endpoints. Because the RIA's endpoints may have spread well outside the office during the pandemic and they may be relying upon different vendors, they should consider the adequacy of their vulnerability management program and consider additional fortification if necessary.

Vendor Monitoring and Testing: As RIAs rely more on third-party service providers, OCIE apparently has increased its due diligence obligations for RIAs. This includes monitoring vendor relationships to ensure that they continue to meet security requirements and notify RIAs about critical personnel changes.

The pandemic may have put overwhelming strain on some of these vendors, and therefore, RIAs may be at risk of a service interruption that could ultimately damage their clients. Therefore, RIAs should consider additional communications with their vendors and evaluation of substitute vendors if necessary.

Risk Assessments: The risk assessment should identify, manage, and mitigate cyber risks relevant to the RIA's business. This includes identification and prioritization of "potential vulnerabilities, including remote or traveling employees or insider threats." In the case of the pandemic, RIAs should assess the increased risks of having its staff working from home or inability to access firm resources as they could at the office. **IA**

Thomas D. Giachetti is chairman of the Investment Management and Securities Practice Group of Stark & Stark, a law firm. He can be reached at tgiachetti@stark-stark.com.

ROBUART/SHUTTERSTOCK