Author
Adam Menkes
Director
Credit Suisse

No Simple Exercise

Risk, not rules, must determine firms' cybersecurity requirements.

The SEC's decision to issue guidance rather than specific requirements around cybersecurity has led to some uncertainty among registered investment advisors (RIAs) over how to implement certain aspects of their cybersecurity programs.

Without a clear statement of their expected obligations, many RIAs report that it has been difficult to determine if they have done enough to satisfy the SEC and investors alike. That said, the majority of firms have formed a strong base and continue to focus on improvements, as the threat landscape continues to evolve.

Over time, the SEC and other regulators have issued substantial guidance on their key areas of focus, and RIAs have realised that taking action based on that guidance rather than waiting for specified regulations is the right approach. In April 2015,[1] the SEC suggested investment companies and advisors "may wish to consider", among other things, risk assessments, a cybersecurity strategy, and written policies and procedures as well as training.

The Office of Compliance Inspections and Examinations (OCIE) initiative in September of that year outlined broker-dealers' and investment advisors' controls.[2]

In addition to the OCIE,[3] regulatory bodies such as Financial Industry Regulatory Authority (FINRA)[4] have provided additional guidelines for managers to look to. While following these other requirements may hold managers to a higher standard than is outlined by the OCIE, there is little indication to date to suggest that the SEC's expectations are lower. Historically, the SEC and FINRA have been quick with enforcement action where their guidelines have been egregiously ignored. The number of cases brought by these two regulators on the basis of cybersecurity failings (at least in part) is already in the double digits.

To each their own

Set in this context, the SEC's lack of specificity gives it the flexibility to evaluate each RIA's adherence to the guidelines independently. The areas where the regulator will spend its time are increasingly clear; encryption, data retention limits, risk assessments, information security policies, documentation, incident response plans and workforce training are all fair game. It seems that there is to be, for now, no definitive or official list of requirements that RIAs can simply check off to claim compliance. In firms where the SEC sees the higher potential risk, it has left itself room to demand greater measures to protect against cyber threats, and lesser measures for threats that pose a lower risk.

1 https://www.sec.gov/investment/im-guidance-2016-04.pdf
2 https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf
3 https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf
4 http://www.finra.org/newsroom/2015/finra-issues-report-cybersecurity-practices-cybersecurity-investor-alert

WHERE DO YOU EXPECT REGULATORS TO FOCUS IN 2017?

Focus Area																	
Answer Options	Accounting fraud	AML/KYC and financial crime issues	Asset misap-propriation	Benchmark and FX manipulation	Bribery and corruption	Client suitability/ misselling	Cyber-security	Fee and expense allocation	Firmwide culture of compliance	High-frequency, dark pools, algo and electronic trading	Liquidity manage-ment	Marketing practices to investors/ customers	Misstating/ misreporting asset values	Proper disclosure for investors	Valuation	Don't know	Response Count
Priority 1	1	34	2	2	5	7	48	16	9	2	8	6	0	10	4	3	**157**
Priority 2	2	17	0	2	4	11	35	19	14	11	7	14	3	9	6	2	**156**
Priority 3	5	11	3	4	12	7	21	7	22	7	5	17	3	18	6	4	**152**

This is not necessarily a bad thing. While RIAs may have less certainty about cyber compliance, they also have an opportunity to look at cybersecurity holistically and pragmatically. This should prompt them to consider not just the regulatory requirements, but also their own cybersecurity risks.

The SEC is rightly focused on investor protection and market integrity. Firms' intellectual property or client lists (from a competitive, rather than privacy, standpoint) are not really its concern. Meeting the SEC standards will not necessarily protect a firm's algorithms, nor retain its customers when a trader leaves. Cybersecurity must go further than minimal compliance satisfaction. To an extent, the SEC's flexibility means that it will continue to determine whether RIAs' cybersecurity controls are adequate on a case-by-case basis, and RIAs likely should be taking the same approach.

GIVEN THE MAGNITUDE OF RECENT CYBER BREACHES, OUR COMPANY PLANS TO FOCUS MORE RESOURCES AND TIME ON CYBERSECURITY.