Papers

Navigating the US Securities and Exchange Commission's evolving expectations for cybersecurity preparedness

Vincente L. Martinez

Erin Ardale Koeppel

Mark Amorosi

Vincente L. Martinez*, Erin Ardale Koeppel and Mark Amorosi

Received: 19th October, 2016

*K&L Gates, LLP, 1601 K Street, NW, Washington, DC 20006, USA;
E–mail: vince.martinez@klgates.com

Vincente L. Martinez *is a Government Enforcement Partner at K&L Gates LLP, which he joined after almost 13 years in regulatory enforcement. He most recently served in the SEC's Division of Enforcement as Chief of the Office of Market Intelligence, and was also a member of the SEC's Cybersecurity Working Group. He also previously served as the first Director of the US Commodity Futures Trading Commission's Whistleblower Office.*

Erin Ardale Koeppel *is a Government Enforcement Partner at K&L Gates LLP. Ms Koeppel defends financial services clients and other companies and individuals in government investigations, regulatory or private litigation and corporate internal investigations. She also counsels clients with respect to corporate governance and compliance matters.*

Mark Amorosi *is an Investment Management Partner at K&L Gates LLP. Mr Amorosi previously served in the SEC's Division of Investment Management, and his practice focuses on investment management and securities law matters involving investment advisers, mutual funds, insurance companies and private investment vehicles, and related issues affecting broker-dealers, administrators, transfer agents and custodians.*

Abstract

The US Securities and Exchange Commission expects its registered broker-dealers, investment advisers and investment companies to implement cybersecurity safeguards through policies and procedures reasonably designed to protect customer records and information, as well as to prepare generally for cybersecurity threats that could undermine the ability to meet regulatory obligations. However, the manner in which registrants are expected to accomplish these goals is uncertain given the SEC's reliance on a principles-based standard, non-specific staff guidance, and the contextualisation of its expectations through enforcement actions. This paper explains the bases of the SEC's approach to cybersecurity preparedness and the challenge of navigating through changing and uncertain expectations, and then offers simple steps to understand and respond to regulatory signals when choosing appropriate cybersecurity measures, as well as memorialising that a firm has acted with the appropriate standard of care.

Keywords: cybersecurity, SEC, guidance, investment, adviser, broker, enforcement

INTRODUCTION

Over the past two years, the US Securities and Exchange Commission (SEC or Commission) has gone to considerable lengths to emphasise the importance of cybersecurity to its registrants, the securities markets and investors. With no hint of hyperbole, SEC Chair Mary Jo White has called cybersecurity the 'biggest risk facing the financial system.'[1] Moreover, since the SEC held its Roundtable on Cybersecurity in March of 2014,[2] its divisions and offices have launched a steady stream of cybersecurity initiatives and efforts:[3] the Office

Journal of Securities Operations & Custody
Vol. 9, No. 1, pp. 6–17
1753-1802

of Compliance Inspections and Examinations (OCIE) announced and conducted two cybersecurity examination sweeps and issued summary findings for the first sweep;[4] the Office of Credit Ratings issued the results of its examinations of ratings agencies, including for cybersecurity preparedness;[5] the Division of Investment Management (IM) issued cybersecurity guidance for registered investment advisers and investment companies;[6] and the Division of Enforcement has brought several cybersecurity-related enforcement actions. As the financial system's cybersecurity vulnerabilities continue to reveal themselves, there is no reason to expect that the SEC's focus on this area will wane. Instead, the SEC likely will continue to concentrate significant examination and enforcement resources on cybersecurity issues.

Despite the SEC's current emphasis on cybersecurity, its expectations are uncertain given that some regulatory requirements are neither clear nor specific, the guidance offered by SEC staff does not have official sanction, and the SEC's examination and enforcement efforts reflect an evolving understanding of the appropriate standard of care. Amid this uncertainty, firms must balance the need to protect customer records and information with a whole host of other regulatory requirements while also balancing competing budgetary demands on their businesses.

This paper explains the SEC's approach to cybersecurity preparedness in the context its Safeguards Rule, draws insights from the SEC's cybersecurity examination sweeps and staff guidance, discusses how the SEC's enforcement efforts are applying an evolving understanding of cybersecurity preparedness and, finally, suggests approaches to navigate through this uncertain regulatory landscape.[7]

INFORMATION SECURITY AND THE 'REASONABLE DESIGN' CONCEPT

A primary goal of cybersecurity preparedness is to protect data from theft, alteration or destruction. While cybersecurity efforts can apply to a variety of functions, threats and forms of disruption, much of the focus of regulators to date has been on data breaches. For SEC-registered broker-dealers, investment advisers and investment companies, the standard for the protection of customer records and information is found in Rule 30(a) of Regulation S-P,[8] known as the 'Safeguards Rule', which states that:

> (a) Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to:
> 1. Insure the security and confidentiality of customer records and information;
> 2. Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
> 3. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Most of the SEC's cybersecurity-related enforcement actions that involve electronic data breaches have been brought as violations of Rule 30(a) of Regulation S-P.[9]

As stated in Rule 30(a), registrants are expected to protect customer records and information through the construction and implementation of policies and procedures 'reasonably designed' to meet the goals of the rule. The meaning of that phrase is not further defined in the regulation. Indeed, while the SEC has previously solicited comments and proposed amendments to provide more specific information handling guidelines under Regulation S-P,[10] those attempts have not resulted in amendments or more specific guidance. Therefore, what remains

to guide registrants is simply the principles-based standard.

The use of the concept of reasonableness as a standard of care and conduct to meet particular goals appears throughout the federal securities laws.[11] As SEC Commissioner Roel C. Campos put it in a 2007 speech to the Luxembourg Fund Industry Association and the American Chamber of Commerce:

> I would also like to dispel the notion that the United States and the SEC are strangers to a principles-based regulatory approach. In fact, the concept of principles-based regulation is not at all new. Broad principles have been set forth in the 1933, 1934 and 1940 Acts as well as in numerous rulemakings. Where possible, we in the U.S. use principles to guide our actions.[12]

However, Commissioner Campos then went on to state as follows:

> Then, our system of enforcement and the court system develop these principles into enforceable rules and standards over time.[13]

Therein lies the dilemma and challenge for firms attempting to meet their regulatory obligations. In SEC enforcement actions under Rule 30(a), the reasonable design concept is applied in a backward-looking manner to determine, in the 'totality of circumstances', whether a registrant acted negligently in light of a reasonable standard of care.[14] As discussed below, the use of a reasonableness standard in the context of a fast-moving technological threat landscape is concerning given that post hoc evaluations of a firm's efforts to comply with Rule 30(a) occur not only in light of the factual circumstances, but also in light of swiftly emerging cybersecurity standards that do not have official sanction and may not reflect industry consensus. While principles-based standards are useful in areas of regulation that require flexibility, they can exacerbate the burden on registrants; ie, it can be difficult, even for firms acting in diligent good faith, to understand what is 'reasonable' at any given time. To put it more plainly, because the reasonable design concept has no solid boundaries, a firm could find itself facing an enforcement action for failing to adopt or consider recent and emerging cybersecurity measures. Moreover, it is fair to assert that the uncertainty created by establishing standards through enforcement actions that apply not only regulatory concepts, but also technological measures, may create unnecessary costs as firms design their cybersecurity programs, not necessarily in light of what is appropriate for their businesses, but rather in light of what they believe will avoid regulatory liability as they try to understand which technological measures regulators believe are appropriate, a fact that they cannot know firmly until regulatory actions have been imposed.

SEC EFFORTS TO COMMUNICATE CYBERSECURITY EXPECTATIONS

Since the SEC held its Roundtable on Cybersecurity, SEC staff have provided firms with information and approaches to enhance their cybersecurity. As explained below, while these are generally positive developments, there are limits on the value of such information because staff guidance carries no assurance that following it will shield a firm from liability. On the other hand, as measures or approaches described in staff guidance become part of the SEC's cybersecurity parlance, a firm's failure to adopt or consider them can become a source of deficiency or liability.

The National Exam Program cybersecurity Risk Alert appendices

OCIE announced cybersecurity examination sweeps in April 2014 and September 2015 through National Exam Program

Risk Alerts.[15] Each Risk Alert contains an Appendix of questions and information requests that firms can expect during an examination. As explained in the April 2014 Risk Alert, the purpose of the attached Appendix is to 'empower compliance professionals with questions and tools they can use to assess their respective firms' cybersecurity preparedness, regardless of whether they are included in OCIE's examinations.'[16] Understanding the Appendix as an act of education is consistent with the stated purpose of the first examination sweep, which was to 'identify areas where the Commission and the industry can work together to protect investors and our capital markets from cybersecurity threats.'[17] Indeed, when the first examination sweep concluded, the SEC published statistics from the examinations, and the Director of OCIE at the time noted that the purpose of the sweep was 'to inform the Commission on the current state of cybersecurity preparedness.'[18]

The April 2014 Risk Alert Appendix, which draws some of its questions from information outlined in the 12th February, 2014 'Framework for Improving Critical Infrastructure Cybersecurity', released by the US National Institute of Standards and Technology (NIST),[19] broadly covers such topics as:

- cybersecurity governance;
- identification and assessment of risks;
- protection of firm networks and information;
- risks associated with remote customer access and funds transfer requests;
- risks associated with vendors and other third parties;
- detection of unauthorised activity; and
- experience with threats.

The September 2015 Risk Alert, which announced the SEC's second cybersecurity examination sweep, also contained an Appendix of questions and requests, which was likewise offered to 'assist firms in assessing their cybersecurity preparedness.'[20] The second examination sweep, however, was intended to be more detailed and focused on controls and implementation. Accordingly, the topics in the second Appendix are more specific, and they identify particular testing records that the examination staff may request, including inter alia:

- information demonstrating the implementation of firm polices and procedures related to employee access rights and controls;
- documentation evidencing firm monitoring for exfiltration and unauthorised distribution of sensitive information;
- information on policies and procedures for managing third party vendors with access to firm networks and data; and
- information regarding the firm's process for conducting tests or exercises of its incident response plan, including the frequency of, and reports from, such testing and any responsive remediation efforts taken.

While the two Risk Alert Appendices are encouraging signs that the SEC's staff are serious about helping firms become more resilient, there are limits to the comfort that firms can take from the guidance. Both Risk Alerts note that the guidance is 'not a rule, regulation, or Statement of the Commission', and that '[t]he Commission has expressed no view on its contents.'[21] Additionally, both Risk Alerts state that the factors cited in the Appendices 'are not exhaustive, nor will they constitute a safe harbor' and that '[w]hile some of the factors discussed in the Risk Alert reflect existing regulatory requirements, they are not intended to alter such requirements.'[22] Further, although the Risk Alerts draw some of their topics and questions from the NIST Framework, neither the Commission nor its staff have endorsed any particular cybersecurity standard.

The Division of Investment Management's cybersecurity guidance

IM issued cybersecurity guidance for SEC-registered investment advisers and investment companies in April 2015.[23] IM staff offered a number of measures that 'funds and advisers may wish to consider … to the extent they are relevant', including:

- Conducting periodic assessments of:
  - the nature, sensitivity and location of collected information;
  - internal and external threats and vulnerabilities;
  - controls and processes; and
  - the effective of the firm's governance structure;
- Creating a strategy to prevent, detect and respond to threats, which can include:
  - controlling access to systems and data;
  - data encryption;
  - restricting the use of removable storage devices;
  - the use of monitoring software;
  - data backup and retrieval;
  - an incident response plan; and
  - routine testing of strategies; and
- Written policies and procedures, employee training and customer education.

Like the OCIE Risk Alerts, the IM staff note that the guidance 'is not a rule, regulation or statement of the [SEC]' and that the SEC 'has neither approved nor disapproved its content.'[24]

The IM guidance goes further than the OCIE Risk Alert Appendices by introducing a broader concept for firms to consider in assessing their cybersecurity preparedness. The IM guidance states that '[i]n the staff's view, funds and advisers should identify their respective compliance obligations under the federal securities laws and take into account these obligations when assessing their ability to prevent, detect and respond to cyber attacks.'[25] IM asserts that cybersecurity threats can affect myriad parts of a firm's overall ability to comply with the federal securities laws:

> Funds and advisers could also mitigate exposure to any compliance risk associated with cyber threats through compliance policies and procedures that are reasonably designed to prevent violations of the federal securities laws. For example, the compliance program of a fund or an adviser could address cybersecurity risk as it relates to identity theft and data protection, fraud, and business continuity, as well as other disruptions in service that could affect, for instance, a fund's ability to process shareholder transactions.[26]

From this language, firms should understand that SEC staff are not thinking of cybersecurity solely in terms of information security, although that is the lens through which the SEC has brought enforcement actions against registrants to date. Rather, the staff are also signalling that cybersecurity failures can undermine a firm's ability to meet any of its compliance obligations, and that firms should prepare accordingly as part of their overall obligation to comply with the federal securities laws.

CASE STUDIES

Below is a discussion of the three most recent SEC cybersecurity-related enforcement actions, as of the date of submission for publication. Despite staff disclaimers that their guidance neither represents the views of the Commission nor modifies regulatory requirements, it is clear that staff-articulated concepts are influencing the SEC's understanding of the appropriate standard of care, which is in turn being applied in enforcement matters.

In the matter of R.T. Jones Capital Equities Management, Inc[27]

In this matter, an investment adviser stored the personally identifiable information (PII)

of retirement plan participants and other persons on a third party-hosted web server, which an intruder breached. The information was not encrypted, but access was limited to two individuals with administrator rights. While the breach 'rendered more than 100,000 individuals vulnerable to theft', there was no indication that any client suffered financial harm, and there was no way to determine if any information was taken. The SEC nevertheless brought an enforcement action, which the firm settled.

The manner in which this matter was settled provides two lessons, one potentially positive and one more concerning. First, it is possible that an immediate and comprehensive response can make a difference in the sanctions sought by the SEC. In this case, upon discovery of the breach, the firm contracted two vendors to learn the extent of the breach, informed its customers, provided identity theft monitoring services, cooperated with SEC staff and implemented remedial measures addressing the circumstances behind the breach. The SEC made note of these facts in the settlement order and imposed relatively modest sanctions; namely, a censure and a US$75,00 penalty.

Second, and more important to understanding the appropriate standard for cybersecurity preparedness, while the SEC found fault with the fact that the firm 'failed to adopt *any* written policies and procedures *reasonably designed* to safeguard its clients' PII' (emphases added), it then went on to enumerate specific failures:

> R.T. Jones's policies and procedures for protecting its clients' information did not include, for example: conducting periodic risk assessments, employing a firewall to protect the web server containing client PII, encrypting client PII stored on that server, or establishing procedures for responding to a cybersecurity incident.[28]

This is a significant illustration of the SEC's approach to evaluating cybersecurity preparedness, given that these particular measures do not appear in a statute or rule. Rather, they are found in post-Roundtable staff guidance.

The citation of these measures should leave firms wary of the prospect that, as cybersecurity standards evolve, SEC staff may borrow and apply new concepts in their analyses as to whether a firm has acted 'reasonably'. This could lead to a perception that the SEC is actively finding fault in a post hoc manner, given that is alleging failures to implement specific defensive techniques in enforcement actions, notwithstanding that relevant SEC regulations do not expressly require firms to implement them.[29] On the other hand, the Commission is not providing the industry with certainty or comfort that the adoption of specific types of measures will insulate a firm from regulatory liability. As the situation stands now, it is therefore very important for registrants to pay attention to SEC staff guidance, statements and enforcement actions, as well as to developments in the industry's thinking on the advisability of particular security measures, because they may become factors for assessing compliance.

In the matter of Craig Scott Capital, LLC, Craig S. Taddonio and Brent M. Porges[30]

In this matter, the SEC found that a broker-dealer violated Regulation S-P because its principals and other employees used personal email addresses to receive faxes that included sensitive customer records and information, as well as by engaging in business communications through personal email accounts. The SEC took issue with the fact that the firm's policies and procedures contained no provisions to address how customer information transmitted through the firm's electronic fax system should be handled. The SEC also found fault with the fact that the firm's policies and procedures contained blanks, including placeholders

for an unnamed designated officer and unspecified methods of protecting customer information. In the resulting settlement, the firm and its two principals were censured, the firm accepted a US$100,000 penalty and the two principals accepted penalties of US$25,000 each.

One notable feature of this matter is that it did not involve a data breach, as has been the case with previous electronic information actions under Rule 30(a). This is significant given that the SEC is focusing on this area in its examinations. As more examinations include cybersecurity reviews, more deficiencies will be found. If the SEC does not consider a breach to be a prerequisite to an enforcement action — or, put another way, if a breach is not seen as necessary to establish a failure to act reasonably — then it stands to reason that enforcement actions may emanate from referrals passed from examination staff to enforcement staff based solely on deficiencies. Therefore, a significant failure to craft policies and procedures reasonably designed to protect customer records and information may lead to an enforcement action rather than simply a deficiency finding.

This matter also illustrates the multiple dangers of using template policies and procedures. While firms are required to have written policies and procedures under Rule 30(a), they must also be 'reasonably designed'. An unedited, untailored template is unlikely to meet this standard.

Ironically, a firm may also be held liable for not implementing policies and procedures included in a template. In this matter, the firm's policies and procedures required the following: the designation of an officer responsible for ensuring compliance; approval by the designated officer for remote access to firm information; the installation of a firewall on the device of any person receiving such information; and that information transmitted to remote devices must be encrypted. The SEC cited the firm's failures to implement these measures. One lesson here is that a firm's policies and procedures must be those actually followed by the firm. Moreover, if a firm is considering a particular measure, it should be added to the firm's policies and procedures only when the firm is ready to implement it.

In the matter of Morgan Stanley Smith Barney LLC[31]

In this matter, a firm employee misappropriated customer PII — including full names, phone numbers, street addresses, account numbers, account balances and securities holdings — and placed it on his personal server, which in turn was likely hacked by a third party. The firm discovered the breach when portions of the customer data began to appear on the internet.

Unlike the cases above, which involved either failure to include certain policies and procedures or departures therefrom, this matter involved an intentional breach by an employee. Nevertheless, the SEC found that the firm violated the Safeguards Rule because its policies and procedures did not include 'reasonably designed and operating authorization modules'[32] to restrict data access to those employees with legitimate business needs, because the firm did not audit or test the effectiveness of its authorisation modules and because it did not monitor employee access to and use of applications from which the information was taken. The settlement included censure and a US$1,000,000 penalty against the firm.

While this matter revolves in part around missing controls, the findings with respect to failures to implement existing controls are particularly noteworthy. This action illustrates that the concept of reasonable design in Rule 30(a) applies not only to the construction of safeguards but also to their implementation.

It is also worth noting that the order mentions that the employee at issue violated

the firm's code of conduct, but it does not credit that fact to mitigate the firm's liability. A firm should not assume that the implementation of a code of conduct will absolve it of a safeguards failure if there are grounds to find that the firm did not implement adequate controls.

APPROACHES TO IMPLEMENTING CYBERSECURITY PREPAREDNESS FROM A REGULATORY PERSPECTIVE

While the regulatory uncertainties described above complicate the goal of achieving compliance, an analysis of SEC staff guidance suggests approaches that, if pursued in good faith, should help firms show that they have acted with the appropriate standard of care. From the simple to the more complicated, a review of the regulatory landscape suggests the following measures and approaches.

First, and most obvious, Rule 30(a) requires 'written policies and procedures'. While much of the dilemma described above revolves around expectations that have no official Commission sanction, this requirement is black letter law. A registrant should therefore be able to produce those policies and procedures intended to protect customer records and information. To the extent that applicable policies and procedures are found in different places in a firm's compliance documentation, such as in its business continuity measures, firm personnel should understand as much and produce those policies and procedures as well.

Second, a firm's policies and procedures should be tailored. The Commission has repeatedly found fault with template or generalised policies and procedures.[33] Chair White amplified this point in her May 2016 remarks at the Reuters Regulation Summit when she stated that '[w]hat we found, as a general matter so far, is a lot of preparedness, a lot of awareness but also their policies and procedures are not tailored to their particular risks'.[34] This is an issue of concern to the staff and the Commission. It also may be a function of the fact that the SEC's focus on cybersecurity has caused some firms to quickly adopt policies and procedures that they have not yet had time to integrate fully into the firm's overall compliance effort.

The level of detail required in written cybersecurity policies and procedures is an important issue with which firms grapple, particularly smaller firms with limited resources. Often, firms have policies, procedures and technologies in place, but do not document them. However, in light of the SEC's emphasis on cybersecurity as a feature of a registrant's compliance programme, documenting cybersecurity practices and technologies should allow firms to easily produce and receive credit for such policies and procedures when requested. In addition, the effort undertaken to create and/or identify such documentation is an important and beneficial compliance exercise.

Third, it is essential, both technologically and from a regulatory perspective, that firms perform periodic risk assessments. Both the IM guidance and the NIST standards referenced in OCIE's April 2014 Risk Alert Appendix note that a risk assessment of cybersecurity vulnerabilities is an early step in creating a well-designed cybersecurity programme. Template or general policies and procedures belie any assertion that such an assessment was performed. Further, as noted above in the discussion of the Craig Scott Capital matter above, the inclusion of policies and procedures that do not accord with a firm's actual practice carry their own dangers.

Further, a thorough, periodic and well-documented risk assessment exercise offers several regulatory benefits. Not every cybersecurity measure conceivable is appropriate for every business. Nor is perfection the expectation. The IM guidance makes

this point clearly by stating that '[t]he staff also recognizes that it is not possible for a fund or adviser to anticipate and prevent every cyber attack.'[35] Accordingly, a risk assessment process that defines those measures that are necessary, appropriate and reasonable for the business — and in doing so defines those that are not reasonable — can serve as a firm's response to examiners in the face of questions and to investigators in the wake of a breach.

Moreover, because regulatory thinking is being informed by technological developments, a periodic assessment should include the input of both operations and legal compliance staff or counsel. On the one hand, a periodic review should consider new technological threats, changes in the firm's business (and therefore its risk profile) and the value of new technological measures. Regulatory concerns aside, the goal of protecting the business requires constant re-evaluation of technologies, threat vectors and techniques.

At the same time, registrants should take time to revisit the regulatory landscape and to survey industry best practices. Doing so will help not only understand the details in regulators' thinking about what constitutes an appropriate standard of care, but it will also allow a firm to create a record of consideration, adoption or rejection of technological measures, that can be provided to regulators to show that the firm was making decisions with reasonable care. While no amount of consideration can ensure perfect cybersecurity, a periodic record of careful consideration, coupled with appropriate documentation, can help a firm demonstrate the reasonableness of its approach.

Fourth, a firm must be responsive when it identifies problems, and it should have an incident response plan in place. Previous SEC cybersecurity actions have involved circumstances where firms ignored vulnerabilities that later led to data breaches.[36] On the flip side, firms that take remedial steps to address issues quickly may receive credit in enforcement actions for those efforts.

Fifth, understanding that the concept of reasonable design encompasses implementation, a firm's policies and procedures should include a set of working controls and regular testing by firm personnel and/or outside vendors. During the course of SEC staff examinations, it is not uncommon for the staff to test registrants' controls. Accordingly, a firm should anticipate that it will be asked to show that its safeguards work by identifying controls and producing testing documentation. Controls testing is also a beneficial exercise for firms because it will help ensure adoption and implementation across the business.

CONCLUSION

While the prospect of pursuing cybersecurity preparedness in an uncertain regulatory environment can be daunting, the approaches described above can help firms meet their compliance obligations. An iterative and periodic approach to risk assessment is a good idea if only because technological threats are evolving constantly. In the course of choosing technological measures to meet identified risks, it also makes sense to revisit the regulatory landscape with a fulsome review that encompasses new regulations, proposed regulations, staff guidance, statements and enforcement actions. As noted above, cybersecurity failures can have unforeseen regulatory consequences. It therefore behooves operations staff, compliance staff and counsel to undertake technological and regulatory reviews together.

References and Notes

(1) Reuters (2016), 'SEC says cyber security biggest risk to financial system', 18th May, available at: http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4 (accessed 17th October, 2016).

(2) Information on the Roundtable is available at: https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml (accessed 17th October, 2016).

(3) Prior to these efforts, in 2011, the SEC's Division of Corporation Finance issued guidance to provide its views regarding disclosure obligations relating to cybersecurity risks and cyber incidents, which are available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (accessed 17th October, 2016).

(4) The 15th April, 2014, 3rd February, 2015 and 15th September, 2015 National Exam Program Risk Alerts are available at: https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert-- Appendix---4.15.14.pdf; https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf and https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf, respectively (accessed 17th October, 2016).

(5) The December 2014 and December 2015 Office of Credit Ratings Summary Reports are available at: https://www.sec.gov/ocr/reportspubs/special-studies/nrsro-summary-report-2014.pdf, and https://www.sec.gov/ocr/reportspubs/special-studies/nrsro-summary-report-2015.pdf, respectively (accessed 17th October, 2016).

(6) The April 2015 Division of Investment Management Cybersecurity Guidance is available at: https://www.sec.gov/investment/im-guidance-2015-02.pdf (accessed 17th October, 2016).

(7) This paper focuses on the obligations of SEC-registered broker-dealers, investment advisers and investment companies. It does not address the separate obligations of registrants subject to Regulation SCI, 17 C.F.R. 242.1000-07, which applies a more specific set of technological resiliency and reporting standards to self-regulatory organisations (SROs), certain alternative trading systems, disseminators of consolidated market data and certain exempt clearing agencies. Also, this paper does not address standards imposed by SROs, including the Financial Industry Regulatory Authority.

(8) 17 C.F.R. 248.30(a).

(9) See LPL Financial Corp., Securities Exchange Act Release No. 58515, Investment Advisers Act Release No. 2775 (11th September, 2008) (settled order finding that firm failed to institute policies and procedures or otherwise act to protect customer information despite internal audit recommendations and despite knowing of breaches through which unauthorised persons accessed, traded and attempted to trade in customer accounts); Commonwealth Equity Services, LLP, Securities Exchange Act Release No. 60733, Investment Advisers Act Release No. 2929 (29th September, 2009) (settled order finding that firm failed to require representatives to maintain anti-virus software on remote computers, nor did firm have procedures to respond to security incidents, which allowed an intruder to access firm systems, obtain customer information and trade); Marc A. Ellis, Securities Exchange Act Release No. 64220 (7th April, 2011) (settled order finding that chief compliance officer failed to revise firm's policies and procedures after laptops and representative's credentials were stolen, which allowed a terminated employee to access and monitor firm communications); David C. Levine, Securities Exchange Act Release No. 64222 (7th April, 2011) (settled order finding that broker-dealer sales manager placed customer information at risk of unauthorised access and misuse by downloading customer accounts to a thumb drive which he removed from the firm); R.T. Jones Capital Equities Management, Inc., Investment Advisers Act Release No. 4204 (22nd September, 2015) (see discussion below); Craig Scott Capital, Securities Exchange Act Release No. 77595 (12th April 2016) (see discussion below); Morgan Stanley Smith Barney

LLC, Securities Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415 (8th June, 2016) (see discussion below); cf. J.P. Turner & Co., LLC, Initial Decision Release No. 395, Administrative Proceeding File No. 3-13550 (19th May, 2010) (administrative decision finding that firm failed to protect hard copies of customer account records, which were found abandoned at the curbside of a representative's former home).

(10) See Next Financial Group, Inc., Administrative Proceeding File No. 3-12738, Initial Decision Release No. 349 (18th June, 2008) at 6–7 and 18–19 for a discussion of previous Commission efforts to amend Regulation S-P.

(11) In one particularly apt example, the concept of reasonable design appears prominently in the standards by which registrants subject to Regulation SCI are expected to establish their policies and procedures. See 17 C.F.R. 242.1001.

(12) Campos, R.C. (2007) 'Speech, principles v. rules', 14th June, available at: https://www.sec.gov/news/speech/2007/spch061407rcc.htm (accessed 17th October, 2016).

(13) *Id*.

(14) See supra note 10 at 22–23.

(15) See supra note 4.

(16) Risk Alert, 15th April, 2014 supra note 4, at 1.

(17) *Id*. at 2.

(18) Press release, 3rd February, 2015, available at: https://www.sec.gov/news/pressrelease/2015-20.html (accessed 17th October, 2016).

(19) The NIST Framework is available at: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed 17th October, 2016).

(20) Risk Alert, 15th September, 2015, supra note 4, at 1.

(21) Risk Alert, 15th April, 2014, supra note 4, at 1; Risk Alert, 15th September, 2015 supra note 4, at App 1.

(22) Risk Alert, 15th April, 2014, supra note 4, at 2; Risk Alert, 15th September, 2015, supra note 4, at 3.

(23) See supra note 6.

(24) *Id*. at 6.

(25) *Id*. at 2.

(26) *Id*.

(27) Investment Advisers Act Release No. 4204 (22nd September, 2015).

(28) *Id*. at 3.

(29) It is worth noting that in one of the few litigated interpretations of Rule 30(a), an SEC administrative court rejected the staff's assertion the Rule required a broker-dealer to encrypt email traffic with recruits while pre-populating account transfer forms. Next Financial Group, Inc., supra note 10. In so holding, the court stated that 'the Commission's authority to compel the encryption of email traffic is nowhere near as plenary as the Division believes.' Id. at 39. More specifically, the court found that because the SEC 'neither established minimum standards nor discussed encryption when it proposed and adopted Regulation S-P', there exists a 'regulatory vacuum' against which 'the Division [of Enforcement] cannot plausibly suggest that NEXT was required to encrypt its e-mail traffic with recruits.' *Id*. at 40.

(30) Securities Exchange Act Release No. 77595 (12th April, 2016).

(31) Securities Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415 (8th June, 2016).

(32) *Id*. at 2.

(33) See Marc A. Ellis, supra note 9, at 3 (criticising 'general and vague' procedures for safeguarding information); LPL Financial Corp., supra note 9, at 4 (finding firm distributed limited and insufficient materials 'and in some instances, only suggestions or recommendations' for safeguarding information); Craig Scott Capital, supra note 9, at 5 (see discussion above).

(34) Supra note 1, at 1.

(35) April 2015 IM Guidance, supra note 6, at 3.

(36) See LPL Financial Corp., supra note 9, at 4–5 (finding that firm did not respond to internal audit recommendations and knew of breaches); Commonwealth Equity Services, LLP, supra note 9, at 4–5 (finding that firm did not respond to evidence of infection of representatives' laptops brought to firm's IT department); Marc A. Ellis, supra note 9, at 4–5 (finding that chief compliance officer failed to revise firm's policies and procedures after laptops and representative's credentials were stolen).