charles SCHWAB

Compliance Review

Ongoing compliance updates for independent investment advisors

April 2020

Advisor Services

IN THIS ISSUE

Pandemic puts business continuity plans to their ultimate test

E.J. Yerzak, CISA, CISM, CRISC, Director of Cybersecurity Services, Compliance Solutions Strategies
Michael Farrell, CISA, CISM, Consultant, Compliance Solutions Strategies
Keith Marks, Executive Director, Compliance Solutions Strategies

I. Introduction

The rapid spread of the coronavirus disease, known to most as COVID-19, reminds us once again of the importance of business continuity planning and testing. Regulatory authorities such as the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and the Commodity Futures Trading Commission (CFTC) will undoubtedly use this event to re-examine, re-emphasize, and re-educate the financial base concerning common weaknesses and lessons learned. In fact, certain regulators have already begun including pandemic-related questions as part of information requests to firms.[1] And beyond the regulatory compliance concerns, many investment advisors are learning firsthand how a disaster or cybersecurity incident could severely impact their service to clients and the stability of their businesses and operations.

The World Health Organization officially declared COVID-19 a pandemic on March 11, 2020,[2] and the United States followed suit with a national-emergency declaration on March 13.[3] State and federal agencies have taken unprecedented actions in the wake of these declarations, including restricting people to their homes and shuttering businesses and schools. For financial firms, these recent events have forced them to rethink how their employees work and how to continue delivering services to clients. The pandemic has put business continuity plans (BCPs) to their ultimate test, and the need for a well-crafted BCP has never been greater.

In 2013, following significant weather-related disasters including Hurricane Sandy, the SEC's Office of Compliance Inspections and Examinations (OCIE) seized the opportunity to remind advisors, broker-dealers, and mutual fund companies of their fiduciary responsibility to clients. This gentle reminder culminated in the "Risk Alert" issued by the National Examination Program (NEP) on August 27, 2013. It is likely that OCIE will similarly focus on how firms have responded to the current pandemic event. Efforts are already underway by SEC staff to gather information

[1] "OCIE Statement on Operations and Exams – Health, Safety, Investor Protection and Continued Operations are our Priorities," Office of Compliance Inspections and Examinations, Securities and Exchange Commission. ("OCIE is actively engaged in on-going outreach and other efforts with many registrants to assess the impacts of COVID-19 and to gather information, including challenges with operational resiliency. In furtherance of these efforts, OCIE may discuss with registrants the implementation and effectiveness of registrants' business continuity plans, particularly in the interests of protecting investors and the integrity of the markets.")

[2] World Health Organization, "WHO Director-General's opening remarks at the media briefing on COVID-19" (March 11, 2020).

[3] Whitehouse.gov, "Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak" (March 13, 2020).

from firms about their business continuity plans, pandemic preparedness, and ability to continue operations for an extended period with a remote workforce. The Examination Priorities Letters and Risk Alerts from OCIE are informative and concise communications that provide items for risk management consideration.[4] We strongly recommend following these communications, which in the past few years have emphasized a variety of technology and cybersecurity concerns that have natural crossover to issues of business continuity planning. FINRA also maintains a simple, user-friendly business continuity plan template that many advisors have used as the framework for their BCP. This white paper begins with a review of the SEC's business continuity practice observations from its 2013 Risk Alert, which still rings true today and takes on an even greater significance in light of the current pandemic. We conclude with a description of necessary and critical steps for advisors to follow when planning for and experiencing cybersecurity incidents affecting their firms.

II. Regulatory basis

The days of arguing the necessity of a BCP are long gone.

The SEC's withdrawal of its 2016 proposed Business Continuity Rule for investment advisors, which included more specific measures around adopting a formal BCP, does not lessen the importance of BCPs as part of an advisor's compliance program. Advisors are reminded that:

> Rule 206(4)-7 under the Advisers Act requires each investment adviser to adopt and implement written policies and procedures reasonably designed to prevent the adviser from violating the Advisers Act. These policies and procedures should include BCPs because an adviser's fiduciary obligation to its clients includes taking steps to protect the clients' interests from risks resulting from the adviser's inability to provide advisory services after, for example, a natural disaster. Under Advisers Act Rule 204-2, advisers have responsibilities to maintain books and records including a requirement to maintain electronic storage media "so as to reasonably safeguard them from loss, alteration, or destruction."[5]

Deficiencies, weaknesses, and to-do items

While there are no known SEC enforcement cases involving business continuity, SEC examinations often include a number of deficiencies that have been reinforced by notions in the alert. Common deficiencies and weaknesses include:

- Failure to maintain a comprehensive list of personnel or the necessary teams and corresponding contact information
- Failure to maintain a list of critical systems and applications indicating essential components of business operations
- Failure to designate alternate personnel for critical operational roles and responsibilities to address key-man risk
- Failure to consider specific regional/geographic threats or scenarios such as inherent weather patterns that could give rise to localized concerns such as storms, flooding, or electrical outages impacting both primary and secondary work locations
- Failure to test the plan, either on a limited or full basis
- Failure to remediate issues and weaknesses identified during testing

Many of these items can be addressed by controls identified by the National Institute of Standards and Technology (NIST) Cybersecurity Framework[6] as building blocks of an effective BCP. Business continuity and incident response concepts are reflected in the NIST Cybersecurity Framework functions of Respond and Recover, taking into consideration response planning, communications, analysis, mitigation, and improvements to the plan.

While such common deficiencies, in isolation or combination, may not represent an enforcement issue, the failure to address identified deficiencies or recidivism across two or more examinations would certainly raise the stakes. It is therefore prudent for advisors to avoid shortcomings and devote resources to mitigating them. The SEC has continued calling attention to this area via numerous deficiencies, and it would not be surprising if an enforcement action occurred around an advisor's business continuity measures—or lack thereof.

Weaknesses noted and simple to-do items

The NEP's Risk Alert of August 27, 2013, discussed six specific weaknesses observed in advisors' plans after Hurricane Sandy. These weaknesses, as mentioned earlier, overlap with some commonly issued deficiencies. The NEP also provided some specific ideas for addressing these issues. The weaknesses fall under three basic categories that advisors, broker-dealers, and financial companies should review, as shown below. We have added three solution steps to the SEC's concerns.

Planning and testing. This includes anticipation of widespread events and the geographic dispersion of resources, and the appropriate testing of all critical operations and systems:

[4] NEP Examination Priorities Letters and Risk Alerts can be found at www.sec.gov/about/offices/ocie.shtml.

[5] "OCIE Risk Alert," Relevant Securities Laws, Rules, and Regulations (August 27, 2013).

[6] NIST.gov, "Cybersecurity Framework" version 1.1 (April 16, 2018).

- Include a regional type of disaster and major disruption in your plan. A natural disaster or event may impact both your primary and alternate work locations if they are on the same electrical grid.
- Ensure that your BCP addresses how your firm plans to continue operating under pandemic conditions. (This item is not currently addressed in FINRA's template BCP; however, pandemic preparedness is identified in FINRA's Regulatory Notice 09-59,[7] which FINRA released in the wake of the H1N1 swine flu outbreak, and it is reiterated in FINRA's Regulatory Notice 20-08,[8] which FINRA released in response to the COVID-19 pandemic.)
- Demonstrate that you have considered geographic dispersion by having redundant backups away from your primary location and a plan for running your business if a regionally or nationally disruptive event occurs.
- Test for the operations/resumption of all critical functional groups and their corresponding systems, even if done on a rotational basis (versus a full failover/failback test). Resumption of critical systems is an important factor to consider when reviewing your BCP in the context of a cybersecurity incident, as your firm will be unable to function if critical systems and data are offline or rendered inaccessible due to ransomware.
- Confirm that critical staff have the resources and access they need to securely operate, for an extended period if necessary, from a remote or alternate location.
- Test your cloud-based systems and virtual private networks (VPNs) to ensure that they can handle the full load of all employees connecting at the same time. Some VPNs may be unable to handle such a load, due to the number of connections or the bandwidth required to support them. Testing here also helps to identify any staff members who are essential to your operations but may currently lack remote access. Document your testing results, make any necessary changes to your IT infrastructure, and be sure to update your BCP accordingly.

Vendors. Conduct due diligence of essential BCP-related vendors, including review of vendors' BCPs, proper maintenance of lists of services and corresponding contacts, and delegation and enlistment of appropriate assistance to and from vendors.

- Put your vendors' BCPs, service level agreements, and any testing available into the due diligence folder. (Review the folder annually and keep it up to date.)
- Make sure the BCP includes your lists of personnel and critical systems. (This is low-hanging deficiency fruit for regulators.)
- If you haven't already done so, create and maintain an inventory of any cloud-based service providers that you use, detailing the types of data stored with each provider, the personnel who have access to the data, and the security controls in place to safeguard the data. Be sure to identify any cloud-based service providers that are critical to your operations, as well as the providers' primary point of contact for your firm.
- Aggregate any testing performed by your key vendors, such as integrity of backups, for your monitoring and validation purposes.

Communications. Ensure that you have considered all essential avenues of communication to both employees and clients.

- Prior to an anticipated disruption, directly contact or send email blasts to clients to ask if they have any immediate needs such as transfers and disbursements that you can process before the disruptive event occurs (a solid suggestion from the SEC). Be sure to maintain current contact information for clients and investors in a readily accessible location.
- Maintain current contact information for all staff and service providers, including emergency contact numbers for all staff.
- If you rely on cell phones and texting as backup for your in-office phone systems, you must ensure that your firm addresses cell phone usage and texting in the context of various recordkeeping requirements. Allowing employees to communicate with clients via cell phone may ease part of the communication burden imposed by having a remote workforce, but your firm must continue to satisfy recordkeeping requirements in order to remain in compliance with the regulations. (Note: While cell phone usage and texting can be part of your backup plan, you should still anticipate the possibility of overall service failure.)
- Use your website or Internet communications to update both employees and clients. You should be able to easily and securely modify your website; that way, you can provide critical communications to clients and investors in the event that you cannot reach them all directly with the speed that may be needed.

Based on the 2013 NEP Alert, FINRA's guidance, and the SEC's direct advice on what not to do, we believe that if you are addressing these basic issues and maintaining your plan, you should be well positioned from a regulatory standpoint.

[7] FINRA, "FINRA Provides Guidance on Pandemic Preparedness," Regulatory Notice 09-59.

[8] FINRA, "Pandemic-Related Business Continuity Planning, Guidance and Regulatory Relief," Regulatory Notice 20-08.

III. Enterprise risk management and governance of information technology

If you are looking for a deeper understanding of business continuity management (BCM), the SEC's mandate for taking into account enterprise concerns is a good starting point. The SEC first highlighted the concepts of "Corporate Governance and Enterprise Risk Management" in the NEP's 2013 Examination Priorities Letter and has continued to focus on these areas, including in the 2020 Examination Priorities Letter.[9]

What do these notions really mean, especially for the majority of smaller advisors, which often consist of two to five personnel?

The SEC has made clear both in publications and in national forums that the enterprise risk management initiative is about ensuring that all firms, regardless of size, are accounting for risks throughout the enterprise, including in operational areas like business continuity and incident management and response. Incident management and response, considered to be a subset of business continuity, addresses business disruptions in the context of a cybersecurity incident such as a malware or ransomware attack. Examiners will speak with upper management in the interview process and assess your firm's culture with questions such as the following: Do you address important operational issues like business continuity across the firm? What is your role in the plan? What systems and controls are in place to help your firm respond to, and recover from, a cybersecurity incident?

Kevin Goodman, the former regional and associate director of the SEC's Denver office, former head of the Broker-Dealer Examination Program, and current National Associate Director of the FINRA and Securities Industry Oversight Examination Program, once stated at an Ascendant conference that enterprise risk management is really about "delegating tasks and responsibilities." The CCO, general counsel, or compliance person facing overwhelming responsibilities in all aspects of the advisory program should consider who can help with the business continuity process:

- Who is the appropriate person from operations to oversee the plan?
- Is there a person in the IT department or at your outsourced IT vendor who can assist with documentation of testing and make recommendations for plan improvements?

Proper management of enterprise risk includes thoughtful and effective assignment of these and other responsibilities.

Smaller firms may actually have it easier here. If your enterprise is not large, you, as a leader, are more likely to be directly involved in continuity efforts. Since BCM, by its nature, takes into consideration the size and scope of operations, regulators may dig deeper into a larger enterprise than they would a smaller firm that has kept it simple (a plan, a backup, and a test).

Action points for Enterprise Risk Management and Governance

- ✓ Consider mechanisms for risk identification and mitigation, such as a risk committee or, at minimum, a program to document the consideration of risks related to business continuity.
- ✓ Maintain a risk matrix, as strongly encouraged by the SEC, and include items under business continuity or risks for disruption.[10]
- ✓ Confirm that your BCP addresses continuity of systems from a technology standpoint, as well as longer-term disaster recovery contingencies such as office relocation and rebuilding from backups. It is critical to have appropriate contact with and understanding of the IT side of the business. Likewise, it is important to communicate with your outsourced IT vendors to understand the potential downstream impacts to your firm of outages or interruptions in the vendors' operations, and to monitor such risk appropriately. Additionally, regular review, testing, and updating of the BCP allows for inclusion of relevant IT personnel in the development and monitoring of technology-related risk mechanisms.

IV. The missing step: Business impact analysis

Whether you are an enterprise or a small business, the steps for BCM and building a plan are largely similar and, in some cases, misunderstood. Most firms simply start with a template plan and begin populating it with information on their current business continuity processes. This makes sense from the standpoint of "papering a file" and may even be encouraged by the prevalence of FINRA's template and off-the-shelf solutions from consultants and law firms. However, this practice tends to bypass a few of the most critical steps, which explains the prevalence of certain deficiencies. By taking the time to conduct a business impact analysis (BIA), your firm will develop BCM procedures that address risks specific to your firm.

[9] SEC Office of Compliance Inspections and Examinations, 2020 National Examination Priorities (January 7, 2020).

[10] The risk matrix has become a standard item in the pre-examination document request.

A BIA has several basic steps that are essential to building your plan:

Perform a vulnerability analysis based on the understanding of your business and the current threat landscape. There are many ways of assessing current threats, including discussing such matters with your peers and aggregating well-known security and breach reports, which often refer directly to threats against specific industry groups.[11] Such a vulnerability assessment is also mandated by certain state laws, such as Massachusetts 201 CMR 17.00, which states that "[i]dentifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks" is part of your obligation to have a written information security program. In light of current events, health epidemics and pandemics certainly qualify as "reasonably foreseeable" external risks that need to be addressed. You must also take into consideration the increase in cybersecurity attacks that inevitably occur when a disaster or pandemic strikes. Documenting such assessments can help you demonstrate to regulators not only that you have considered these risks, but also that you continually monitor and review them in light of the requirements of the Compliance Rule 206(4)-7.

Create an inventory of all systems and services from which you will determine what systems and operations can and will continue in the event that offices must be closed for an extended period. Seasoned advisors take this matter seriously and keep this information in a readily accessible spreadsheet or database. It may make sense for CCOs, in conjunction with a firm's head of IT or a consultant, to perform this task based on functional groups (portfolio management/trading, operations, finance and accounting, client relations, etc.). This inventory will serve as the basis for your list of critical systems and services to be included in your plan.

Based on the priorities of your critical systems and services, determine the order in which services are restored and the approximate recovery-time objective (the amount of time from outage to restoration) and recovery-point objective (the point in time from which data can be recovered if there's a disruption). Periodic testing should be conducted with your IT department or IT vendor to ensure that recovery point and time objectives are current and reasonable; understanding these two items will give you an idea of how long your systems may be offline in the event of a cybersecurity incident. For cloud-based systems, ensure that service level agreements define a minimum uptime: a guarantee that online services will be available for a certain amount of time, usually expressed as a percentage (e.g., 99.9% uptime). Such determinations and objectives are specific to your business model. For example, a private equity firm with a small number of portfolio-company investments held on a long-term basis may not require the same speed of recovery as an actively managed hedge fund that transacts frequently and uses leverage.

The BIA and each of these steps, if properly performed based on the size and scope of your business, will serve as the building blocks of your BCP. Also, the assessments built into the BIA process must be reviewed annually to meet regulatory expectations that the plan will be updated annually based on the results and lessons learned from your testing program.

V. Testing

If there is one place in which advisors and broker-dealers tend to struggle, it is the understanding and execution of testing. This is another area in which scope of business is material. For example, advisors and financial services companies that are application providers—or whose investment models are based on quantitative or computing-intensive processes—tend to treat testing as important. They view continuity as essential to their core business and tend to employ best practices regarding business continuity as a means of reducing business risk. Regulatory concerns are not the primary driver for such firms. But asset managers and smaller firms that use systems and services of broker-dealers and custodians in a highly automated environment tend to view business continuity as primarily a regulatory compliance matter and want merely to meet the minimum regulatory requirement. This attitude is understandable given limited resources, time constraints,

Looking for more information on compliance or regulatory issues?

Schwab's compliance website includes a searchable database, compliance tools, and many other resources to assist you. Visit schwabadvisorcenter.com > News & Resources > Compliance. (See "Online compliance resources" on back page for more information.)

[11] See Verizon, Microsoft, and Cisco.

and increasing regulatory demands. But considering the governmental responses to the COVID-19 pandemic, with states shutting down and people being required to stay home, a "do the minimum" attitude has likely impacted current performance for some firms and could hinder performance in response to a similar event in the future.

One misconception we hear repeatedly in the industry in response to questions regarding testing is that a snowstorm or hurricane tested the plan. But a risk management plan based upon waiting for actual events to occur is a recipe for disaster, whereas proactive and regular testing can help find weaknesses and improve the plan before disaster strikes.

To be sure, the way your firm weathers actual storms (or navigates through other disruptive events) is important. But regulators are likely looking for evidence that you have designed and implemented testing in *anticipation* of such events, rather than simply using the most recent disaster as the only testing you conduct. Your firm may have been able to endure prior weather disruptions, but was it prepared for the unforeseen consequences the latest pandemic has presented? Each test, whether planned or unplanned, can present opportunities to learn which aspects of the plan worked well, which did not work as intended, and, more importantly, what infrastructure and communications changes can be made going forward to maintain the ability to continue operations. Another common weakness is the sole reliance on vendor testing as evidence that a firm is testing its plan. While such information is good supporting evidence for the due diligence, BCM, and monitoring processes, the SEC will want to see that you, your key personnel, and perhaps management are all participating in line with enterprise risk management expectations.

One misconception we hear repeatedly in the industry in response to questions regarding testing is that a snowstorm or hurricane tested the plan. But a risk management plan based upon waiting for actual events to occur is a recipe for disaster, whereas proactive and regular testing can help find weaknesses and improve the plan before disaster strikes.

Action points for testing

- ✓ **Start modestly; any testing is better than none.** A "call tree" test is a simple way to establish that alternative communications (text message, email, and cell phone communication) are working properly. Have employees document their participation and any failures. Two other tests that are fairly easy to complete are (1) an "Internet failover" test, assuming you have a backup provider, and (2) a "phone rollover or forwarding" test in the event that your phone service cuts out and backup provisions forward telephone calls to designated locations or numbers other than the primary.
- ✓ **There is a regulatory expectation for "full test" of your plan at least once a year,** which might include the assumption that your primary business address is unavailable and that all operations must be conducted remotely (with partial or entire staff working from home for an indefinite period) or migrated to your determined disaster recovery site. You should also test your firm's ability to respond to a cybersecurity incident, during which a critical system may be taken offline for hours or days due to malware or ransomware. We believe this full test can be accomplished in stages and by rotating key personnel and functional groups. In other words, get as close as possible to this expectation and document your efforts appropriately.
- ✓ **Verify server backups and test resumption capabilities frequently.** Ensure that your IT department or IT vendor is verifying that backups complete successfully, and have them perform a full system restore periodically. Backups have probably been tested from time to time when an employee inadvertently deleted a file, but restoring a file is a different animal than restoring an entire server from a backup because of a cybersecurity incident. Validate that the recovery point and recovery time objectives defined in your BCP are correct, and adjust them if necessary.
- ✓ **Write it up.** No matter what type of testing you are doing, or even if you're merely aggregating from vendors, make sure you document it properly: dates, objectives, personnel, results, and lessons learned. Keep in mind that the purpose of testing is to identify potential gaps in your program and ultimately improve the BCP. Take the opportunity to document disruptions and analyze results. Our experience is that regulators are primarily concerned with whether you have a process and the ability to prove it. The documentation of testing need not prove that all plans functioned flawlessly. Rather, testing should be viewed as an opportunity to discover gaps in plans. Those gaps, when identified, should be remediated via updated procedures within the BCP, and those procedures should be tested at the next opportunity. The purpose is to improve continuously, not to be perfect in the first test.

VI. The cloud

The reality of geographic dispersion and the fact that many advisors are now using at least some cloud-based systems (G Suite, Office365, etc.) give tacit acknowledgment that cloud-based solutions offer real benefits, especially in the face of mandatory lockdowns and work-from-home orders. Cloud service providers offer scalable solutions for both large advisors at the upper end of the technology food chain and small advisors looking for reasonable and cost-effective alternatives.

Many IT directors and personnel who resist cloud services do so out of fear of letting data leave the perimeter. But most cloud vendors encrypt data while it's both in transit (being used) and at rest (not being used) on their servers. They also encrypt backups using industry standard protections. Encrypted data is secured and protected from prying eyes. Some internal program leaders are still hesitating on this issue because they fear performance degradation and have particular business needs requiring that their data be maintained in-house. Embracing cloud services means escalating due diligence to another level, and the SEC has suggested that firms review vendor infrastructure and ensure appropriate dispersion of data (making sure your data is not stored next door). Most cloud-based service providers have data warehouses spread throughout the country to ensure that your data is available wherever you are and whenever you need it. In the event that one facility is disrupted, the data is available immediately from a redundant site in another location that is not experiencing the same disruption.

The major questions regarding cloud-based providers are as follows:

- What should we, as users, do to test the security of these environments?
- How can these environments be hardened from a security standpoint, such as by confirming that default passwords have been changed and that network ports are open only if necessary?
- Will the firm's data and systems be safe and accessible via the cloud?

Remember the old compliance saw: "You can outsource the process, but you cannot outsource responsibility."

This principle would, of course, also apply to vendors' services that are specific to business continuity. After all, stipulations of Regulation S-P and the obligation on the part of advisors to provide reasonable physical and logical security for client information clearly extend to business continuity services and operations. It may be true that large cloud vendors provide a bigger bull's-eye for hackers and "advanced persistent threats,"[12] but many of these same providers also have the resources to survive on the cutting edge of security and testing.

The movement to cloud-based solutions is therefore worth considering, as necessary, in the context of BCM and ongoing due diligence.

Cloud providers have changed continuity planning in ways that can help advisors and other financial service companies achieve objectives. Benefits and capabilities are numerous, but the following may be key to BCM considerations:

- Comprehensive email/communications, document creation, sharing, and versioning through such solutions as Microsoft 365 and G Suite for Business, among others.
- The use of specific web-based applications for CRM, compliance, archiving, monitoring, portfolio management, client portals, code versioning and development, etc.
- Providing online access to custodial websites to place trades and process money movement requests.
- The ability to accomplish backup in a certified (SSAE-18) environment, which may provide security controls and monitoring that are otherwise difficult or impractical for many businesses.
- Flexibility with respect to deployment models ranging from private cloud and managed hosted models to full virtual services and public or shared-tenant environments. (Understanding these models and terms of data ownership, transference, and destruction are standard service level agreement items and due diligence responsibilities.)
- The ability to manage other critical services such as internal and external chat and videoconferencing systems.

Searching major cloud vendors under the subject of business continuity shows that this is an area in which vendors are focused and offering a variety of solutions that may help firms meet various requirements.[13]

Visit Schwab's Cybersecurity Resource Center

Schwab Advisor Services has resources available to help you strengthen your cybersecurity program, including educational materials, actionable tools, and third-party resources. The resource center also contains a white paper focused on helping you develop a customized business continuity plan. Visit schwabadvisorcenter.com to access these resources.

[12] "Advanced persistent threats" implies a threat by an organized group or even a governmental entity that may target high-profile organizations or companies through a number of techniques with the goal of gaining access to, attacking, or stealing specific information.

[13] See, for example, RackSpace.

VII. Cybersecurity incident management and response

Incident management is "the capability to effectively manage unexpected disruptive events with the objective of minimizing impacts and maintaining or restoring normal operations within defined time limits."[14]

Public and business consciousness of security breaches has never been higher. Data breaches continue to be big media events and the type of public relations disasters that mean tangible business risk. The COVID-19 pandemic has created new opportunities to prey on remote and distributed workforces via phishing attacks and cyberattacks on videoconferencing systems.

Financial companies are being compelled to address this business risk not only by the threat of unwanted media attention, but also by the demands of institutional clients and regulators through requirements like Regulation S-ID, which requires advisors meeting certain definitions to have an identity-theft prevention program in place in order to detect red flags and prevent or mitigate identity theft.[15] In other words, and at least with respect to identity theft, advisors must have an incident management and response program that lays out the set of actions a firm will take in response to a cybersecurity incident. Moreover, FINRA and the SEC have continually identified cybersecurity as a focus area in their Regulatory and Examination Priorities Letters in recent years. FINRA's 2020 Priorities Letter states that "... FINRA will thoroughly assess whether [firms'] policies and procedures are reasonably designed to protect customer records and information consistent with Regulation S-P Rule 30," realizing that controls should be appropriate to firm business models and the size of their businesses.

While the management of specific IT-related incidents may not trigger a full-blown business disruption, the possibility cannot be discounted, and your BCP should take into account the possibility of IT-related security events. All 50 states now have some sort of data breach notification law in effect, which was not the case when regulators first began reviewing cybersecurity as part of their examinations. Furthermore, several states appear to be following the General Data Protection Regulation (GDPR) model in designing their own data privacy requirements.

Massachusetts, one of the first states to mandate specific data protections for its residents, is now joined by states such as New York (with its New York Department of Financial Services Cybersecurity Regulation, as well as its SHIELD Act) and California (with its California Consumer Privacy Act, or CCPA). The CCPA largely mirrors the privacy rights conferred on EU residents under the GDPR. It includes provisions such as requiring covered firms to respond to consumer requests to provide the data they have collected regarding the consumer and to delete such data upon request, unless an exception applies. The CCPA also drastically expands the definition of "personally identifiable information" for California residents.[16] Advisors to California residents must now include these factors in the definition of "personal identifiable information" that will trigger reporting obligations in the event of a breach. Additional states are moving in a similar direction in terms of adopting stronger data privacy requirements, leaving a patchwork of standards in their wake for organizations with clients in multiple states.

Cybersecurity best practices in the current environment

Review the Schwab resource "Cybersecurity best practices during the COVID-19 outbreak" to ensure that your firm is taking additional precautions to protect your clients.

[14] ISACA, Certified Information Security Manager (CISM) Review Manual 2012, USA, 2011.

[15] The Rule Release for Regulation S-ID requires advisors subject to the rule to perform due diligence of third-party service providers with respect to issues of identity theft. This would apply to any vendors that provide solutions and environments in which personal information of clients and employees must be protected, including BCP-related service providers (see page 54 and footnote 120).

[16] California Legislative Information, SB-1121 California Consumer Privacy Act of 2018 (published September 24, 2018).

Action points for developing cybersecurity incident management and response plans

Incident management and response can be viewed as a subset of business continuity management because an incident, such as a ransomware attack that locks all of a firm's files, is certainly a business disruption. Cybersecurity frameworks are great resources for developing and updating business continuity and incident management and response plans. One such framework, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, allows firms to take a risk-based approach to the controls they implement. The framework is organized into five sections—identify, protect, detect, respond, and recover—each of which details the specific issues that plans should address. When developing your incident management and response plan, keep the following in mind:

- ✓ Remember that your incident management and response plan is a key component of BCM, and the lack of such a plan will be fuel for future deficiencies.
- ✓ Similar to a BCP, your incident management and response plan should have roles assigned and clear steps to follow (planning and preparation, detection and analysis, containment recovery, post-incident analysis, and lessons learned).
- ✓ Test your incident management and response plan for specific scenarios, such as a critical server being infected with ransomware, and then document and aggregate results with BCP testing.
- ✓ Plan for the worst in the form of a security breach that leads to declaration of an emergency or disruption as defined in the BCP, with potential media, legal, and law enforcement involvement.

VIII. Conclusion

The landscape of BCM continues to change based on enabling technologies, regulatory initiatives, and the demands of institutional clients.

Accepted principles of change management should be applied to both business and IT environments. The most important adjustments in firms' BCM processes will likely emerge through consideration of regulatory and security issues with respect to new services and providers. While this white paper has provided a broad swath of information on issues raised in regulatory risk alerts and on some other areas vital to business continuity, the subject is vast, and many topics call for elaboration.

In its annual Examination Priorities Letters, the SEC continues to address business continuity concepts indirectly under the themes of protecting clients' personal information and continuity of operations as a fiduciary. Firms should use the COVID-19 event as an opportunity to ensure that their BCP specifically addresses health epidemics and pandemics. An up-to-date BCP will identify all the processes and systems in place that will allow a firm's employees to continue servicing client needs in the event they are forced to work remotely for an extended period.

Advisors can apply only what is reasonable to the efficient conduct of their own operations. In other words, use a common-sense approach that:

- Provides for annual review of your process and plan
- Tests and records as feasible
- Considers the best interests of your clients

Even the smallest firm should apply an analytical and best-practice approach to BCM. Finally, we note one last key aspect of BCM that goes hand in hand with testing: good training. When done properly and with the support of management, training that emphasizes the importance of continuity can contribute to the culture of compliance and security at your firm.

About the authors

E.J. Yerzak, CISA, CISM, CRISC
Director of Cybersecurity Services
Compliance Solutions Strategies (CSS) /
Ascendant Consulting Services

E.J. assists advisers to hedge funds, private equity funds, funds of funds, pension advisers, and retail investment advisers in bridging the gap between compliance and cybersecurity risk management. In addition to conducting compliance program annual reviews, risk assessments, and mock exams, E.J. is the director of Cyber IT Services of the technology team at CSS, which provides cybersecurity consulting services to its clients. In this capacity, E.J. assists firms in assessing and managing their cybersecurity risk, from network vulnerability scanning and penetration testing to onsite cybersecurity assessments and assistance in implementing the NIST cybersecurity framework.

E.J. has authored articles and alerts on emerging regulatory and technology issues, and is regularly requested to speak as a cybersecurity expert at industry conferences and events throughout the country. He is a Certified Information Systems Auditor (CISA®), Certified Information Security Manager (CISM®), and Certified in Risk and Information Systems Control (CRISC™).

E.J. holds a Bachelor of Arts in both English and computer science, magna cum laude, from Colgate University; a Master of Science degree in computer information technology from Central Connecticut State University; and a J.D., magna cum laude, from Quinnipiac University School of Law. He is licensed to practice at the State Bar of Connecticut and in federal court before the U.S. District Court for the District of Connecticut.

Michael Farrell, CISA, CISM
Consultant
Compliance Solutions Strategies (CSS) /
Ascendant Consulting Services

Michael Farrell is a consultant within CSS's Shield Cybersecurity division and is responsible for conducting cybersecurity risk assessments, policy gap analyses, vulnerability scanning, penetration testing, and social engineering testing. Mike's IT background includes experience in network installations and management, hardware and software configuration, and troubleshooting.

Mike holds a Bachelor of Science in Accounting from Central Connecticut State University and is a Certified Information Systems Auditor (CISA®) and Certified Information Security Manager (CISM®).

Keith Marks
Executive Director
Compliance Solutions Strategies (CSS) /
Ascendant Consulting Services

Keith is involved in the management and distribution of Compliance Solutions Strategies' (CSS) products and services. He works across CSS to find regulatory data and reporting solutions that investment managers need. Keith manages a team of directors, consultants and compliance managers in CSS's Ascendant compliance services team, which provides consulting, annual compliance program reviews, risk assessments, on-site mock examinations, registration services, and cybersecurity services to institutional wealth managers, private fund managers, retail wealth advisers, and registered investment companies. He also helps coordinate educational conference agendas and speakers.

Keith is an author, product contributor, and thought leader. His product contributions have included the design of Ascendant's FREE Form ADV Part 2 Template distributed to over 6000 advisers in 2010-12, and his vision of compliance program management built into the Ascendant Compliance Manager. With his colleagues, Keith's most recent significant publication is "Big Data, Using Data Analytics," Modern Compliance vol. 2, ch. 23 (2017). Keith also is one of the lead designers of CSS's Form CRS Automator.

Keith joined Ascendant Compliance Management in 2007, and Ascendant became a part of CSS in 2016. Prior to Ascendant, Keith was an instructor for the Center for Compliance Professionals and Director of Investment Adviser Services at National Regulatory Services (NRS). Keith practiced law previously as an associate with Day, Berry & Howard LLP (now Day Pitney LLP), a Hartford, Connecticut law firm, in 1996-98. Keith served as a law clerk for two years in Connecticut's Supreme Court and Appellate Court after earning his J.D., magna cum laude, from Western New England University School of Law and his Bachelor of Arts, magna cum laude, from the University of Connecticut. He is a member of the State Bar of Connecticut, and is actively involved in raising funds for the Polycystic Kidney Foundation (www.pkdcure.org).

Keith served as President of the New England Broker Dealer Investment Adviser Association (NEBDIAA), a nonprofit organization, incorporated in 1997, from 2012-17. He has been on the Board of Directors of SOAR Educational Enrichment, Inc. since 2013, and Board Chair since 2015. SOAR is a privately funded 501(c)(3) providing educational enrichment programs to Keith's local elementary school.

Online compliance resources

Visit schwabadvisorcenter.com > News & Resources > Compliance for compliance and regulatory information.

Schwab works with third-party firms to provide select resources that help keep you informed of certain regulatory and compliance developments. Access *Compliance Hot Topics*, templates and guideline documents, archived issues of *Compliance Review*, and third-party resources. These resources are complimentary and exclusive to advisors who work with Schwab Advisor Services™.

JUT (0420-0HJF) NWS108530Q2-00 (04/20)

charles SCHWAB

Own your tomorrow®