THOMSON REUTERS
Westlaw®

Business continuity planning: preparing for pandemics and other significant business disruptions

By John Sakhleh, Esq., and Chris Mills, Esq., *Sidley Austin LLP*

JUNE 22, 2020

Broker-dealers and investment advisers operate in environments that are full of risks. Every day, these firms consider a host of risks when making investment decisions, such as market risk, credit risk, and counter-party risk. Along with managing investment risks, firms frequently pay close attention to reputational and regulatory risks that may affect their business.

Appropriately accounting for these types of risks can be what distinguishes well-performing firms from the competition, so it should be no surprise that firms often devote substantial resources to hiring personnel, developing systems, and creating a culture to manage these types of risks.

But as the current COVID-19 pandemic shows, less typical risks also can significantly affect firms. Firms should, consistent with relevant regulatory obligations, have plans in place to deal with events that may significantly disrupt their normal operations.

This article provides an overview of the regulatory obligations for broker-dealers and investment advisers to have business continuity plans that are reasonably designed so that the firms can continue to operate in periods of disruption and addresses topics firms should consider when developing those plans.

REGULATORY REQUIREMENTS TO HAVE BUSINESS CONTINUITY PLANS

Broker-dealers and investment advisers are required to have plans to deal with significant business disruptions. For broker-dealers, FINRA Rule 4370 principally mandates that they "create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption."

These procedures "must be reasonably designed to enable the member to meet its existing obligations to customers" and "must address the member's existing relationships with other broker-dealers and counter-parties." This requirement is principles-based, and firms generally have flexibility in designing and implementing a BCP that is tailored to its business.[1]

For investment advisers, the U.S. Securities and Exchange Commission considers the adviser's fiduciary duty to include a requirement to have a BCP.[2] Further, the Commission expects advisers who are required to register with it to account for issues related to emergency preparedness when designing and implementing policies and procedures pursuant to Rule 206(4)-7.[3]

In practice, the topics that an adviser should consider when developing a BCP are similar to those identified by FINRA.

As a result, even though the particular rules applicable to broker-dealers and investment advisers are not identical, and although firms may comply in a number of different ways, the fundamental obligation is essentially the same: A firm must have a BCP that is reasonably designed to prepare the firm to operate during significant business disruptions.

DEVELOPING A TAILORED BUSINESS CONTINUITY PLAN

Constructing an appropriate BCP requires a comprehensive assessment of a firm's operations to identify risks the firm may face.[4]

Constructing an appropriate BCP requires a comprehensive assessment of a firm's operations to identify risks the firm may face.

Once risks have been identified, firms should attempt to develop resilient systems that address them and permit continued operations in a variety of challenging environments. Indeed, the ability of a firm to operate in difficult environments can be heavily attributed to proper planning, stakeholder awareness, and investments in systems.

There is no one-size-fits-all BCP, but reasonably designed BCPs frequently address a number of topics, such as the following.[5]

MONITORING THREATS

Firms should have a framework in place to identify and monitor threats that may disrupt aspects of their operations.

Often, alerts and guidance from federal agencies, such as the Department of Homeland Security and the Center for Disease

Control, non-governmental organizations, such as the World Health Organization, and state or local governments can be particularly informative.

Firms should consider developing relationships with these types of organizations to facilitate the timely receipt of relevant information. Depending on a firm's size, it may also be appropriate to have a team dedicated to monitoring for threats and alerting management to potential disruptions.

Firms that rely principally on guidance from the federal government or international organizations should assess whether to incorporate guidance from more local authorities. In some circumstances, guidance from institutions such as the WHO may not accurately reflect local conditions, and therefore it is more appropriate to base decisions on guidance from local authorities.

Along with monitoring for threats, firms should have a framework in place that addresses how to respond.

Generally, a firm should use flexible guidelines to determine how to implement its BCP in a way that appropriately reflects that many events can trigger aspects of a BCP, and the severity of those events can vary. This may include using a tiered approach that activates different aspects of the BCP based upon the severity of a disruption.

ALTERNATIVE WORK ARRANGEMENTS AND INCREASED ABSENTEEISM

A significant disruption may dramatically affect the ability of employees to work from their normal place of business. In some circumstances, like natural disasters or terrorist attacks, disruptions may be limited to only some of a firm's offices.

In other instances, such as pandemics like COVID-19, the affects may be much more widespread. Given the variety of circumstances that could limit access to normal places of business, firms should consider how to continue operating while access to one or more of its offices is either restricted or not possible. Firms should also address the possibility that a significant disruption may prevent some employees from working, even remotely.

There are a variety of ways to address the risk that a firm's normal place of business may not be fully operational. For example, firms may maintain secondary or back-up sites, transition responsibilities to offices that remain open, or implement remote-work arrangements.

For firms with back-up or satellite offices, firms should consider whether there are certain types of disruptions where those locations will not be sufficient, such as if the secondary location is near the normal location. An event that restricts access to the firm's main office may also restrict access to the secondary location. Further, firms should consider whether the layout of a secondary office location may not permit sufficient social distancing during pandemics — an issue that some firms may be currently experiencing.

REMOTE WORK ARRANGEMENTS

Given the possibility that employees may not be able to work from either their office or secondary locations, a BCP should also address remote-work arrangements. The ability of employees to work remotely largely will depend on their access to telecommunications networks and other infrastructure.

Firms therefore should proactively consider the possibility that an employee's residential internet connection may not be functional or may not be sufficient to permit the employee to meaningfully work from home.

To mitigate these risks, firms should consider how to best ensure that critical employees — including employees performing key control functions such as compliance, risk management, back office operations, and financial and regulatory reporting — can access telecommunications networks while working remotely.

Potential options include providing personal hotspots, ensuring that residences of critical employees are serviced by a back-up ISP, or securing space at locations (such as hotels) close to the residences of critical employees. Firms also should consider installing back-up generators at homes of key personnel to ensure connectivity and continuity of operations.

> There is no one-size-fits-all BCP, but reasonably designed BCPs frequently address a number of topics.

Employees working remotely may face more cyber-related risks, as they may not be protected by corporate firewalls or other systems that firms usually use to protect their information systems. Further, cybersecurity risks associated with data privacy and data security may increase because attackers may try to breach systems while IT personnel and support functions are facing increased demands.

These attacks can take many forms, including, for example, phishing, installation of malware software such as ransomware or spyware, or password attacks.

To help fortify against potential cybersecurity risks, firms should, among other things, provide personnel with secure connections to the work environment (e.g., through a virtual private network (VPN) using multi-factor authentication) and provide personnel with training and information for increased awareness of potential scams and other attacks. For example, firms should consider providing alerts or

reminders concerning phishing attempts, fake calls, or client impersonations.

Firms also should consider whether its supervision systems should be modified while employees are working remotely.[6]

Determining whether a supervisory structure is reasonably designed will depend largely on the firm's particular business, and firms should consider whether their supervisory policies appropriately take into account the different functions of different employees. For example, it may be appropriate to use policies and procedures to remotely supervise traders or portfolio managers that differ from the policies and procedures used to remotely supervise analysts.

Firms should also assess whether their remote supervision procedures address concerns that may be more prominent while employees work remotely, such as those involving cybersecurity or capturing communications or other records. Among other things, employees working remotely may be more likely to use online collaborative or communication tools, including some programs that would not usually be used if the employees were not working remotely.

> Firms should consider whether they are appropriately capturing and reviewing electronic communications.

As a result, firms should consider whether they are appropriately capturing and reviewing electronic communications and other records relating to their business while employees are working remotely.

ABSENTEEISM

Even with the best planning, in some circumstances it may not be possible for certain employees to work, even remotely. This absenteeism can present risks to a firm's ability to perform functions if institutional knowledge is limited to particular personnel.

To mitigate these risks, firms should consider cross-training employees or creating guides or other training materials that can be used so other personnel can temporarily fulfill the obligations of absent employees.

RELATIONSHIPS WITH THIRD-PARTY SERVICE PROVIDERS

An event that significantly disrupts aspects of a firm's operations may also disrupt the operations of third-party service providers that the firm relies upon for compliance, operational, technological, telecommunications, custody, and other services. Given the importance of these providers to a firm's ability to serve its clients or customers, firms should assess the ability of vendors and suppliers to deliver continued services during emergencies.

Indeed, testing the ability of service providers to support a firm during disruptions — and developing plans to shift to other providers if necessary — can be critical to operating during a crisis.

To that end, firms should:

- periodically review the scope of existing arrangements and service levels with key vendors such as clearing firms, custody firms, banks, telecommunication providers, and compliance service providers;
- determine whether vendors have adopted their own BCP and, if so, review the BCP to understand how the provider will respond to significant disruptions;
- maintain an updated list of key service providers and the relevant contacts, with contact information so the providers can be reached during a pandemic or other disruption;
- consider including in future agreements (or amending existing agreements) a requirement that the service provider test its BCP annually and report the results;
- review the geographic location of vendors and assess whether key vendors are located in the same region as the firm or each other;
- review provisions of agreements related to termination rights, force majeure clauses, service level arrangements, and default provisions to help plan for situations where the vendor is unable to perform the contracted services; and
- maintain a list of alternative vendors or suppliers in case existing vendors are unable to provide the contracted services.

COMMUNICATING WITH EMPLOYEES AND THIRD PARTIES

Communicating with personnel, clients, vendors, and other third parties during a pandemic or other disaster is imperative. Accordingly, firms should have a plan on how to contact and communicate with its personnel and others, including identifying which firm personnel should execute and implement the firm's communication strategy.

Firms should consider preparing sample messages in advance of an event so that communications can be quickly disseminated to personnel, vendors, and other third parties should a disruption occur. To increase the likelihood that personnel will receive updates or alerts, firms should have personnel review and update their personal contact information so that the firm can communicate, among other things, office closings and updates/status of the firm's operations.

WEBSITE UPDATES AND EMAIL COMMUNICATIONS

To the extent feasible, firms should provide updates, as needed, on the firm's website or by email communications to customers or clients. Similarly, firms should send reminders to employees regarding best practices during disruptions, including those related to cyber-security and record management.

The ability to communicate electronically will largely depend on access to functioning telecommunications infrastructure and, as discussed above, firms should also take steps to ensure their service providers will be able to continue operating during a significant disruption.

CALL CENTERS

Even with regular updates to a firm's website, a significant disruption may lead to significantly more calls from customers — many of whom may be affected by service outages or limitations. Accordingly, a BCP should consider how to best provide uninterrupted connectivity to its call center.

An assessment of systems capacity for handling client inquiries should be undertaken to determine if existing infrastructure can handle high call volume and how calls would be routed if call-center employees worked remotely.

If existing call centers in the United States need to be expanded, firms should consider contingency plans for hiring additional personnel during a market disruption to address the high call volume. These plans should consider the possibility that an event that significantly disrupts the firm's normal operations may also affect the firm's ability to promptly identify, hire, and train new employees.

If a firm's normal call center is overseas, the firm's BCP should address how that call center's functions can be shifted to other locations, including the United States. Shifting the location of services or hiring additional personnel may raise registration issues and questions about the necessary supervisory structure and training, and firms should have a framework in place to deal with these types of issues as they may arise.

CONTACT WITH REGULATORS

Firms should also assess their ability to promptly contact regulators during a crisis. Regulators may, for example, be able to provide guidance on how other market participants are responding or no-action or similar relief in situations when a firm may be under unprecedented stress.

TESTING

Creating a BCP is only the first step in the process for planning for significant disruptions. Firms should also develop and employ a controlled testing strategy to confirm that their BCPs are reasonably designed to be appropriately tailored to the firm's business.

Importantly, these tests should be designed to reflect the types of disruptions the firm is reasonably likely to face. Properly conducted, testing provides opportunities to anticipate and address issues before they cause operational problems. Indeed, regulators have remarked that firms that conduct meaningful tests have historically experienced minimal disruptions when significant events occur.[7]

There are a number of ways that firms may conduct testing. Firms may use tabletop scenarios (*e.g.*, personnel review their processes in a conference room and describe their role in the event) or full-scale simulations (*e.g.,* personnel participate in walk-through scenarios).

Regardless of form, tests should assess functionality of systems the firm may rely on during a significant disruption (including back-up technology or those used in remote-work arrangements), the accessibility of secondary locations, and the ability to function in the absence of certain personnel.

Testing should also account for the fact that a significant event may also stress a firm's liquidity or reserves. Further, firms should assess how a significant disruption that occurs close to regulatory-reporting deadlines may affect the firm's ability to meet its regulatory obligations.

Firms should also assess which personnel should participate in testing. At a minimum, it is likely that testing should involve critical personnel, as they may be involved in implementing the BCP and may be most familiar with the firm's operations. At the same time, firms should consider rotating personnel involved in testing, both to obtain a set of fresh eyes that may detect gaps or identify areas of potential improvement and to cross-train employees.

In this regard, testing can provide additional training for handling disruptions. In many circumstances, it may also be appropriate to include key counter-parties or service providers in testing, to familiarize all parties with how they each plan to respond to disruptions.

The frequency of testing will likely depend on the size of firm, continuity of key personnel familiar with the BCP, and complexity of the business. At a minimum, firms should consider annual testing, with increased testing if there are changes to key personnel, systems, or regulatory requirements.

Firms should document the results of testing and promptly address areas that warrant attention. Any changes to a firm's BCP should be promptly communicated to personnel and relevant third-parties.

CONCLUSION

Regulators expect firms will conduct their own analysis to identify and mitigate risks related to pandemics, severe weather, or other events that could significantly impact a firm's operations, and meeting these regulatory requirements requires effective coordination and planning.

Firms that devote appropriate resources will be best positioned to prepare for, respond to, and recover from significant disruptions.

NOTES

[1] Rule 4370 identifies ten topics that a broker-dealers BCP should address, "to the extent applicable and necessary." They are: (1) data back-up and recovery (hard copy and electronic); (2) all mission critical systems; (3) financial and operational assessments; (4) alternate communications between customers and the member; (5) alternate communications between the member and its employees; (6) alternate physical location of employees; (7) critical business constituent, bank, and counter-party impact; (8) regulatory reporting; (9) communications with regulators; and (10) how the member will assure customers' prompt access to their funds and securities in the event that the member determines that it is unable to continue its business.

[2] *See* Final Rule, Compliance Programs of Investment Companies and Investment Advisers, Release Nos. IA-2204; IC-26299, 68 Fed. Reg. 74,714 at 74,716 (Dec. 24, 2003); *see also* Proposed Rule, Adviser Business Continuity and Transition Plans, Release No. IA-4439, 81 Fed. Reg. 43,530 at 43,534 (July 5, 2016).

[3] *See supra*, n.2.

[4] *See, e.g.*, FINRA, Business Continuity Planning FAQ #16, https://bit.ly/2YMRwR4

[5] This article does not address every issue that could be relevant to a business continuity plan. It does not address, for example, what steps to take to secure offices from physical threats. Rather, this article highlights some areas that may be of particular regulatory focus in the current environment.

[6] *See* FINRA, *Transition to Remote Work and Remote Supervision*, Regulatory Notice 20-16 (May 2020).

[7] *See* FINRA, *Business Continuity Planning*, Regulatory Notice 09-59 (Oct. 2009); NASD, *Business Continuity Planning*, Notice to Members 06-74 (Dec. 2006).

This article appeared on the Westlaw Practitioner Insights Commentaries web page on June 22, 2020.

ABOUT THE AUTHORS

John Sakhleh (L) is a Washington-based partner in **Sidley Austin LLP**'s securities enforcement and regulatory group. **Chris Mills** (R) is a senior associate who is also based in Washington and serving in the firm's securities enforcement and regulatory group. This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The content therein does not reflect the views of the firm. This article reflects the situation at the time it was written based on the rapidly changing nature of the COVID-19 pandemic.