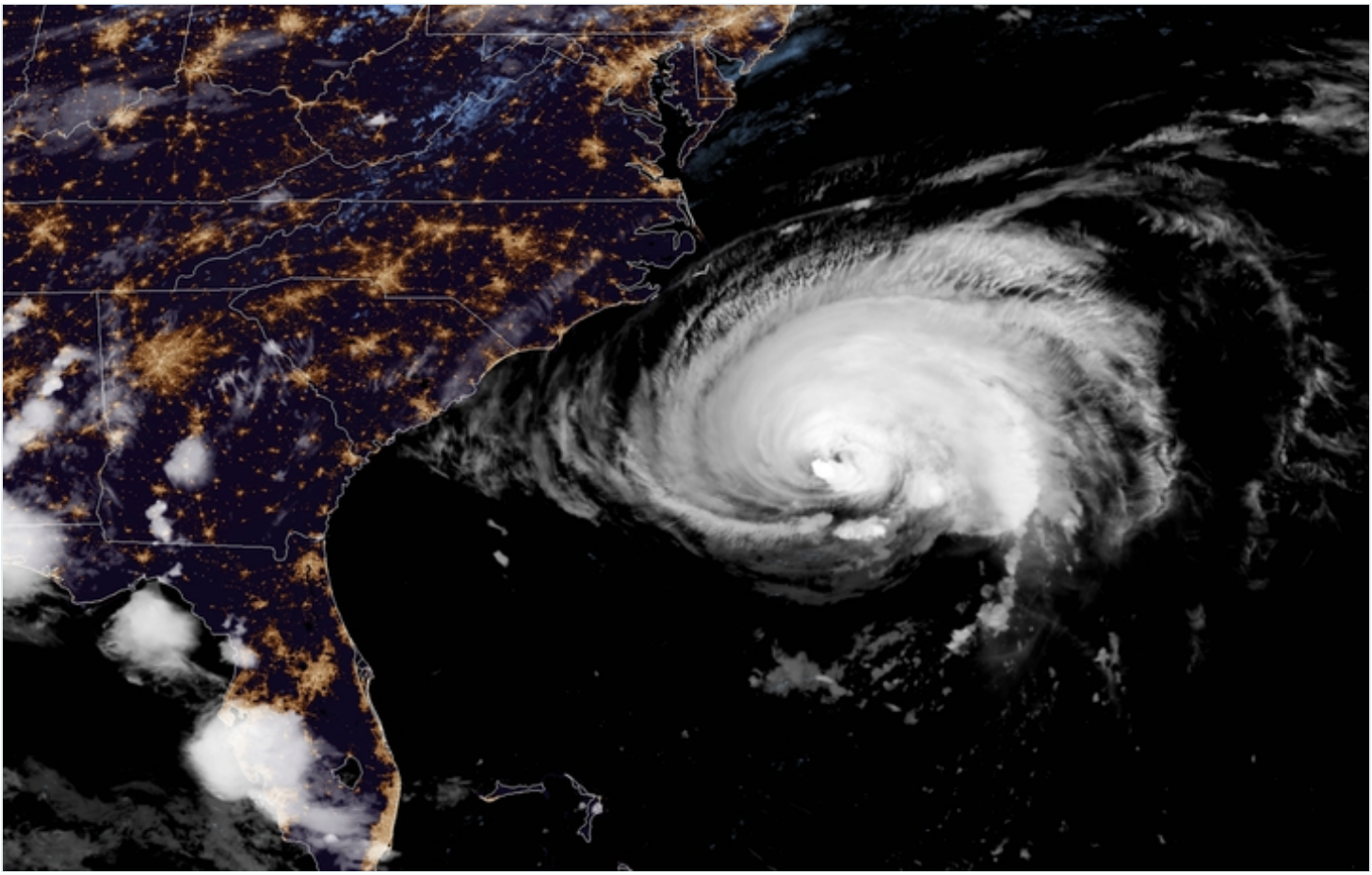
compromise data, result in lost business or prevent employees from accessing a physical office. How quickly will your firm be ready to seamlessly continue operations?

May. 15, 2020



The next disaster – a new epidemic, data breach, earthquake or flood – could compromise data, result in lost business or prevent employees from accessing a physical office. How quickly will your firm be ready to seamlessly continue operations?

We have all experienced a change in the way we work. As all or most employees work

A business continuity plan includes a series of protocols designed to ensure that operations can keep functioning during a disruptive event. A disaster recovery plan addresses the steps and technologies for recovering from a disruptive event, including recovery of lost data, or repairing failed systems or technologies. The following measures should be included in your business continuity and disaster recovery plans:

- **Transparency with Firm Employees.** Knowledge is power when it comes to bouncing back from a crisis. It is crucial that the firm be transparent about the current health and security risks.

- **Communications to Clients.** Share the steps and technologies that the firm is using with your clients so they understand that your firm is prepared and the trusted advisor relationship is protected. Encourage all clients to use the firm's secure portal to share documents and reports.

- **Clear Terms of Service and Privacy Policy.** All firms today need to have clear terms of service and privacy policies in place that inform clients how their personal data and information are managed and protected. Part of those policies should include a clear statement of the firm's remote work protocols and protections.

- **Location of Data.** Recovery plans require convenient access to data, so you must know where and how your data is stored at all times. Easier access comes from having your data stored in the right manner, so you should think ahead and only work with providers that keep your data in jurisdictions that ensure compliance and make the most sense for your firm and client base.

- **Data Segmentation.** Employing data segmentation practices in advance will help with continuity and recovery. Using a private cloud isolates your data from the data of other companies, because you're not sharing infrastructure when you are in a

public multitenant cloud. Data mirroring, or the practice of maintaining exact, real-

- **Around-the-Clock Support.** A seamless remote work environment will require access to technical support for all of the systems, applications and products you use. Because you can never predict when a breach or disruption might happen, it's critical that providers offer 24/7 support.

- **Immediate Failover Capabilities.** In computing, failover is a process for switching to a standby or redundant technology if a server, system, network or program is compromised or otherwise made unavailable. If you can't afford any downtime, you need to make sure you have immediate failover capabilities in place across the board to ensure continuity.

- **Backups.** Having backups for networks, systems and other technology is critical to ensuring continuity and avoiding downtime, but they're only useful if you know they work. You should not only be making a point of regularly backing up your data and systems, you should also regularly test and verify your backups to make sure they'll function when you actually need them.

- **Termination.** If you need to terminate the use of a technology or a relationship with a provider due to a breach, you need to have clear processes in place. Among other things, they should guarantee a timeline for recovering any compromised data and make clear who owns that data after termination.

The immediate need to support remote work has brought with it an increasingly complex and risky landscape in ensuring your firm's data is safe. Thinking proactively about business continuity and disaster recovery now will ensure your firms data is safe today and you are ready for future disasters and WFH scenarios that may occur.

========

Tomas Suros is a technology advocate working at the intersection of IT and client