riskfocus

WHITE PAPER

Crises as Change Agent: From the TechWreck to the COVID-19 Pandemic

riskfocus

Executive Summary
In the first two decades of this century, we have witnessed several crises that have dramatically changed the way businesses are run and have pushed most companies to an ever-increasing reliance on technology. In this article, we look at practices and technology changes that COVID-19 is forcing onto Capital Markets businesses. These include the impacts due to “work from home” mandates, the unanticipated and challenging new security considerations, and the specific demands on Capital Markets systems.

The COVID-19 pandemic will inevitably have a drastic impact on companies and their cultures, but steps can be taken to alleviate some of the pain and to address the acute problems. These include steps to get everyone connected and communicating, to make or accelerate plans for migration to the cloud, and to accelerate the automation journey.

Background

The September 11 attacks challenged many long-standing assumptions on growth and security, forcing changes in the way many companies operated. Following September 11, US financial markets closed for several days as significant critical infrastructure in downtown New York was either destroyed or inaccessible. These events spurred a renewed focus on business continuity planning by both enterprises and regulators. After September 11, no large financial institution could justify ignoring the possibility that one of its primary sites could become inoperable.

The global financial crisis of 2008-2009 led to remarkable changes in Wall Street’s regulatory and technology landscape; regulators reined in trading desks that had previously been unfettered, where risk was either unmeasured or measurement was broken. The crisis exposed the limits of complex risk models, which had failed precisely at the moment they were most needed. The fallout was so significant that, in the years since 2008, the primary task for technologists in the financial industry has been implementing technology to meet more stringent regulations.

The global financial crisis also left banks in a weakened state, ripe for Silicon Valley to begin entering domains that were once the sole province of Wall Street. As bank developers focused on regulation, Silicon Valley sprinted ahead with innovation. That process continues, with several pieces of core financial infrastructure moving to SaaS platforms developed by technology companies (e.g., payments processing).

The COVID-19 pandemic is more like September 11 than 2008, in how it is affecting the broad economy as well as government behavior in a way that most certainly will match or exceed the impact of the September 11 attacks. In addition, the pandemic is exposing faults and fault lines in the assumptions around work, security, and safety, while testing business continuity processes like never before.

COVID-19 Impact: Culture and Risk Management

Cultural Change

The COVID-19 pandemic is the first crisis that has compelled nearly all workers to work-from-home, on account of government- and/or company-imposed self-isolation. The most visible impact on firms has been through work-from-home policies. Prior to the outbreak, most financial institutions had tentatively and gradually allowed staff to use most office productivity software and some core banking/trading functions remotely, connecting back to the office over VPN. The pandemic has exploded VPN-use, and many firms have had to allow employees to use applications from home that were previously prohibited. In the Capital Markets industry, this includes core applications such as institutional trading as well as payments and settlement systems.

Working from home has systems and infrastructural considerations, but it also has a strong cultural component. Many companies have relied on face-to-face meetings and proximity to decision-makers to be able to run their businesses. They are not only ill-equipped at having the right remote collaboration software, but more importantly, they do not have the processes that allow decision-making and execution to happen seamlessly.

Security and Process Risk

The impact of the COVID-19 crisis has depended to some degree on a company's preparation prior to the pandemic. For example, institutional traders are finding that home networks are not as fast or reliable as those on site and have therefore changed their trading patterns. These changes are occurring in an environment where all aspects of global markets are experiencing unprecedented, prolonged market volatility that will continue for weeks, months, or even longer as the impact of COVID-19 reveals itself on each segment of a country's economy.

For much of the financial services world, the prospect of all employees working remotely raises several unanticipated security considerations. The previous model, for many in the field, was a central office protected by high walls, with remote users being the exception.

However, in a world where there is no office and many connections are made via SaaS or point-to-point, any entity that depends mainly on a perimeter defense needs to re-evaluate its stance. Further, with tens of thousands of computers enabled to run even the most sensitive of applications, perimeter defense is a non-starter. Organizations that have not already done so will have to move to an in-depth defense strategy with layers of security protecting each level. Organizations lagging in encrypting all their traffic and data are at a much higher risk of being compromised.

In addition, a technology shift will, in our view, be accelerated by the pandemic. Most banking enterprises were already moving towards standardizing workloads and operations with containers, taking the first exploratory steps towards a public cloud. The end goal of containers is to enable portability, maintainability, and scalability of compute workloads, an objective that dovetails with migrating workloads to public clouds. Banks that have long run data centers with small, focused teams are suddenly confronting the prospect of staff taking ill at the same time. For an enterprise reliant entirely on one or two physical locations, this prospect can be devastating to operations.

Market and Credit Risk
Each financial segment has been impacted in a unique way, but common themes include:

- Exchanges, Liquidity Providers, ATS, Inter-Dealer Brokers, and sell-side trading desks have a sudden need for more infrastructure to handle spikes in volumes without compromising trading latency and throughput
- Central counterparties need to monitor risk and margin in real time, which requires elastic grid computing to run pricing and risk models
- Buy-side institutions—hedge funds and traditional institutional asset managers—require the same type of elastic grid computing for risk calculations and portfolio simulations

In general, any entity responsible for managing financial risk will have to modify its base case to include “fat tails,” or extreme events.

- Extreme market dislocation, which has occurred roughly every ten years, needs to be part of any stress test
- Rolling, industry-wide counterparty defaults and force-majeure scenarios need to be mainstreamed
- Systems that were unable to handle spikes will require re-engineering

The financial markets consist of enormously complex machinery that assumes that certain relationships are unchanging. These correlations and specific behaviors can and do completely breakdown when there are big dislocations. For example, treasuries and traditional safe havens such as precious metals generally go up when stocks go down. During the last weeks of March, as the pandemic intensified, all assets dropped precipitously as long-standing correlations between asset returns were undone. In some cases, higher quality assets fell faster than others since they were the only ones readily saleable in a flight to cash.

Then, as fiscal and monetary policy measures were enacted, most assets rose sharply. The only way to navigate such uncertainty is to plan actively for more extreme scenarios and by using “non-normal” (i.e., fat-tailed) distributions, which treat outliers as first-order possibilities rather than footnotes. Such planning requires the elastic computing power provided by the cloud, allowing increased computing resources to be tapped and released as necessary.

Due to the pandemic, more companies will move to utilize the cloud, which will likely spawn more regulation. There will be a need for bigger, better, and cheaper systems but also a need for smarter ones. The chief benefit of the cloud is not that it simply provides raw elastic compute power but, rather, that it provides higher-level building blocks as a service. This infrastructure allows new applications to be launched in weeks and months rather than years. It also allows for sophisticated pattern matching, machine learning, and AI algorithms to be put in place. The current IT setup in many organizations means than many will struggle with the rapid changes brought about by the COVID-19 pandemic. In contrast, organizations that have embraced the cloud and its resources are prepared to further extend their advantage of adapting to change quickly.

What Next

It is imperative that the financial services industry transitions to this next generation of cloud-based technology and adaptive practice once the acute phases of the COVID-19 pandemic pass. Much like earlier crises, the effects of the pandemic will likely last for years, with strong secondary effects setting in once the initial impact has subsided. To summarize:

- The pandemic highlights the need for distributed organizations and processing.
- Thus far, our industry has focused on physical threats as failures of single locations and infrastructure. We are quickly confronting the fact that multiple, geographically separated locations can fail simultaneously.
- People may be the most vulnerable link, and a highly compartmentalized, single-point-of-failure organizational chart is also a great risk.
- Organizations with flexible, automated workload deployment and scaling will be able to move these workloads around public cloud provider data centers to avoid outages; no single person, team, location, or region can be singularly critical.
- Those stuck with manual, custom/tribal processes will face far higher risk if a team takes ill or if a geographic area is affected by a government-mandated shutdown.
- Legacy systems designed for structured, predictable, and batch processing are ill-suited for addressing major market disruptions.

The steps to take are clear:

Address the acute problems: get everyone connected, get everyone communicating. Solutions such as AWS VDI, Zoom, and Slack can accelerate this tremendously (full disclosure: Risk Focus uses all of these).

Start making plans (or accelerate plans) to migrate to the public cloud. If, for example, AWS loses a data center or a region, they have 70 availability zones in 22 regions; that is more redundancy than any enterprise can hope to build on its own. It is worth noting that our clients who have already moved to the public cloud are in much better shape than those who have not, both for the immediate reason that they can easily access their data and workloads, as well as the less obvious reason that they have adopted the processes and methods allowing them to use the cloud effectively. When single individuals or small teams hold tribal knowledge that can be lost, people become the weak link. These methods—automation, agile development, freedom within strong guardrails—are well-suited to a distributed workforce and are very resilient in the face of adversity.

Address the ever-increasing complexities on Risk and Trading Platforms. Risk and Trading systems must be re-architected to deal with intense market volatility, which can drive huge spikes in volumes; increasing complex calculations, which demand access to massive amounts of previously siloed data; and systems that can process these complex calculations in near real-time. Organizations and systems must be equipped to respond to rapid changes that are unlikely to dissipate.

Learn More

At **Risk Focus**, our business is to help overcome challenges like these. We help firms with tactical response, moving workloads and data to AWS; we also work with clients on strategic response, creating migration plans, creating landing zones, and starting DevOps and Cloud transformation with concrete steps that benefit our clients. We can help with initial assessments; security reviews re-architecture and migration of business-critical applications (e.g., trading, risk, reporting) and infrastructure (e.g., streaming systems, data-rich systems).

We are proud to be a part of the large partner ecosystem offered by AWS. AWS offers a variety of financial incentives for organizations that are just beginning their cloud journey as well as those for organizations that are well on their way with cloud technologies.