Perspectives on Industry Resilience

By Andrew Gray, DTCC Group Chief Risk Officer

SIFMA Operations Conference
April 15, 2015

Introduction

Good morning, I am pleased to have the opportunity to be here at SIFMA Ops 2015. It is exciting to see how this conference has continued to evolve over the last few years and remains a key event for the industry to share ideas, collaborate, build professional networks and forge consensus on important topics we face. This morning I want to focus on risk management and my perspectives on industry resilience.

Key Topics

To share some of my background, I spent the past 5 years overseeing DTCC's Systemically Important Financial Market Utility or SIFMU businesses, and during that time I had the opportunity to witness and help respond to the evolution and transformation of risk management. Risk management is at the heart of our mission at DTCC, and for more than 40 years, we have helped protect the stability and integrity of global financial markets. We have also seen risk management evolve tremendously over these past four decades, but the 2008 financial crisis was an inflection point that changed the risk paradigm for the industry. It ushered in a new era of greater regulatory scrutiny, and as a result, risk management has emerged as the top priority for the industry and policymakers – and I would argue that it is a key determinant in our ability to increase investor confidence in our industry.

It is in my relatively new capacity as Group Chief Risk Officer for DTCC that I want to share with you my views about how risk management has evolved – and will continue to evolve – in the coming years by focusing on three topics this morning:

- One, how the remit of risk management organizations has expanded in recent years,
- Two, how this expansion leads to the increasing need to take a systems view in thinking about risk, and
- Third, the importance of broadening the industry's view of risk management with the goal of building more resilient systems.

And finally, I will conclude by looking at key challenges and opportunities we face to achieve these goals.

Expansion of the Remit of Risk Management

First, let's talk about the expansion of the scope of the risk management organization. Like many companies in the industry, we have expanded the remit of Risk Management at DTCC over time from a focus on credit, market and liquidity risk to now include operational risk, systemic risk and, most recently when I assumed responsibility for the Risk team, Technology Risk Management, Physical Security and Business Continuity Management.

There are several reasons for the expansion of the role:

- First, there is a recognition that firms can be brought down by a wide variety of incidents. In our case, a technology outage, operational breakdown or cybersecurity incident could be devastating to us as well as to the larger industry.

- Second, it helps establish clearer distinctions between policy definition and risk assessment from execution and day-to-day management, particularly in the case of technology and information security risk.
- Third, there is a need for a holistic view of risk and a consistent approach to measuring and managing risk across multiple risk types.
- And, fourth, there is a need to understand the connections between and among various risk types because issues in one risk family can have a knock-on effect in other risk categories.

The Need for a Systems View in Thinking About Risk

I want to talk in more detail about this idea of interconnections because it is critical to taking a systems view in thinking about Risk. In financial services today, there is increased complexity and unpredictability in the nature and impact of the risks that we must be prepared to defend against. As a result, I believe we need to look at the financial system not as a set of stand-alone entities, but rather as a complex, adaptive system with a set of diverse interconnected components, with multiple feedback loops between them and where risk is distributed across the system – and sometimes not in a transparent fashion.

Expanded Boundaries

This systems view has many implications for how we need to think about managing risk. Importantly, we can no longer restrict our views to what happens inside the four walls of each of our institutions. Given the interconnections and heavy dependencies between institutions that make up the financial ecosystem, one must have an understanding of the extended enterprise, including other financial institutions and market participants, their clients as well as vendors and even vendors of vendors.

For example, vendor risk is a fairly new area of focus, but it is critical because, as we have seen in recent times, vendors or vendors of vendors can pose a significant threat to an organization. The recent cyber-crime against Target illustrates this point – hackers appear to have accessed the firm's systems by launching a malware-laced email phishing attack on a HVAC company that contracted with the retailer.

In addition to vendor risk, we also need to better understand our points of connection with other entities, including the activities of the clients of our clients.

Many firms are working on ways to meet these requirements, such as the International Securities Services Association (ISSA) which is engaging with its members, including us at DTCC, to develop principles for addressing the need for further transparency in the custody value chain.

We have watched these and other similar developments very closely at DTCC, and they have helped to shape and inform our thinking as we have enhanced and strengthened our own risk management practices. For example, we formed a Systemic Risk Group a few years ago to conduct outreach and engage with regulators to identify and report on internal and external sources of systemic risk.

These efforts have yielded many benefits, including helping us produce an interconnectedness analysis. This analysis extends DTCC's risk management focus to risks that arise from key entities to whom DTCC is connected to or reliant upon for critical services, such as settlement banks, clearing banks and other financial entities. We feel that this analysis on interconnectedness represents an important development in risk management for "systemically important financial institutions" (SIFI). In fact, the Office of Financial Research performed an analysis similar to DTCC's by rank ordering the riskiness of SIFI's by measuring the degree of interconnectedness risk each poses.

Shifted Time Horizon

While having a view of the extended enterprise is important for the reasons I just explained, we also must adjust the time horizon in which we view risks.

Many of you may know the famous George Sanatyana quote, "Those who do not remember the past are condemned to repeat it." This best summed up the risk time horizon of yesterday in that we often looked to the past to predict the future. However, with systemic risks emerging more quickly and with greater complexity than ever before, the past is no longer a complete or accurate barometer on future risks. Today, a better quote might be: "Past performance does not necessarily guarantee future results."

As a complex, adaptive system, financial markets will sometimes behave in ways that are difficult to predict, especially if we are using tools that assume linear behavior or are based on normal statistical distributions. In other words, we need think about the unthinkable, and adjusting the time horizon to take on a more forward-looking view that enables us to place greater emphasis on mitigating extreme but plausible risks.

Firms recognize this need to understand and define extreme but plausible events, and many are working on scenario analyses across their organizations. But importantly, these analyses need to extend beyond the traditional credit or market risk factors examined in stress test exercises today to also include scenarios for operational or technology incidents, such as cyberattacks.

One other characteristic of our modern financial system that I want to note is that it is open and more susceptible to attacks and threats. The reality, combined with the diversity of the threat environment and the unpredictability that I mentioned earlier makes it inevitable that we will have to deal with breakdowns in service.

Broadening the View of Risk Management—Building System Resilience

What does this mean for our industry? Let me turn to my third point and explain why we must broaden the view of risk management to also focus our efforts on building greater system resilience.

We all know it is important to measure, analyze and mitigate risk, but given the inevitability of a breakdown, firms also need to be able to detect the problems and recover as efficiently and effectively as possible, minimize contagion and ultimately learn from these events.

Of course, DTCC has a long history of advancing initiatives that will reduce risk and improve resilience in the industry and our markets, but I would like to share with you our experience with building resilience within our company and its operations.

Risk Ownership/DTCC 3.0

There are a number of building blocks to strengthening resilience, but I believe one of the cornerstones is establishing a strong risk culture and expanding ownership of risk management to all employees of a firm. Several years ago, we did just this at DTCC. We began an enterprise-wide culture change initiative, known as DTCC 3.0, to embed risk management into all parts of the organization. This effort required much more than investing significantly in risk management and other control functions or developing new risk-based technologies. It demanded that we change the mindset of the organization and establish a new framework for thinking about how all our employees perform their jobs.

While DTCC has always had strong controls and processes in place, our goal was to look with a fresh set of eyes at everything we do for its potential to cause systemic risk. To accomplish this, we empowered and incented employees to act as risk managers, we integrated risk management goals into year-end reviews and development plans, and we encouraged employees to speak up when they saw something that raised alarm. We have made tremendous progress over the past several years, but we view this as an ongoing journey that has no end because we know we must never lose focus on mitigating risk.

"Managing the Unexpected"

There are many other ways in which organizations need to evolve to build systems resilience. I recently had the opportunity to read an excellent book on this topic that offered valuable guidance, and I want to share some of the key takeaways with you.

The book is "Managing the Unexpected – Resilient Performance in an Age of Uncertainty," by Karl Weick and Kathleen Sutcliffe. It was originally written in 2001 and it describes a set of core principles for building resilience based on approaches taken by what are called High Reliability Organizations (HROs).

Examples of HROs that were examined in the book include nuclear aircraft carriers, air traffic control systems, emergency medical treatment teams and wild land firefighting operations. Needless to say, these HROs operate in a space in which errors could lead to disastrous consequences.

Even though financial market infrastructures such as DTCC were not explicitly included in the types of firms that were analyzed, I would suggest that, given our role in the industry, we would be classified as an HRO, and I believe many of the lessons from the book are instructive for us and the financial industry more generally.

The five core principles for creating High Reliability Organizations are as follows:

Principle #1: Preoccupation with Failure – This is a mindset in which everyone in the organization is always looking at what could go wrong. Just because the impact of an actual incident may be minor, it doesn't necessarily mean that we're safe. HROs examine each small failure to see if it indicates problems with the larger system.

Principle #2: Reluctance to Simplify – There is a danger in oversimplification that can lead to skipping or hiding critical details that could be the Achilles heel of an operation.

Principle #3: Sensitivity to Operations – While strategic direction is important, one must stay attentive to the front line where the real-time work is being done, including paying attention to close calls or near misses where the front-line has the most knowledge about such events.

Principle #4: Commitment to Resilience – This must be developed and maintained through ongoing preparations and deliberate testing so that an organization can adapt to changes, remain operational during periods of stress and bounce back from a crisis and learn from it.

Principle #5: Deference to Expertise – In a crisis, authority should migrate to the people with the most expertise, regardless of hierarchy. Knowledge and experience won't necessarily follow the organization chart, and it is important that key decisions are made by those with the proper experience and expertise.

There is one final point that the authors stress – the importance of "mindfulness" or being fully aware of what is going on and, in particular, learning the lessons of past crises. We believe developing this learning mindset throughout the organization is a key component of building a risk and resilience culture so let me take a moment to share with you several examples of what we are doing at DTCC to implement some of these principles.

Last year, we formed a Business Resilience working group comprised of senior executives from multiple areas. While there was a lot of activity going on around the firm in different areas, we wanted to ensure that we had a comprehensive, coordinated view of what was happening, that we were bringing the best thinking to the table and sharing ideas, and that we were providing guidance and making progress on the highest priority items.

The group identified a number of work streams that fell into this category, such as the formation of a Post Incident Review Team (PIRT). While we do very detailed post-mortem analysis on all incidents that affect our operations, we believed it was important to get a senior group of employees together from not just technology and operations, but people with different backgrounds and responsibilities across the firm in order to look at the incidents from many different perspectives. The PIRT is responsible for looking at what else could have happened if certain controls were not in place; understanding how an incident in one area could affect other areas; and related to this, generating themes that are broadly applicable to the organization.

In addition to this, we also expanded our view of incidents to include near-misses because we felt that we could learn from these events rather than just breathing a collective sigh of relief that we dodged a bullet.

The work of the PIRT is a great example of how we are implementing the principles of Preoccupation with Failure and

Reluctance to Simplify because we are probing beyond the initial technical analysis of root causes for incidents while ensuring that we keep the folks who are at the front-line engaged.

What we learn from these incident reviews also helps us better understand other potential situations that we may face, which, in turn, is directly relevant for another high priority effort that is being coordinated by our Operational Risk Group, scenario analysis. This reflects our ongoing Commitment to Resilience and understanding of where we need to rely on Expertise.

DTCC's scenario analysis helps management experience how events could potentially play out, how existing processes would hold up and what actions would have to take in reaction to, or to prevent these events from happening.

An added bonus in running scenarios is that they can help to pinpoint key-person risk or reliance on areas outside ones organization for expertise because as companies expand, turnover and new markets may create vulnerabilities.

In addition, we are also going a step further than just conducting hypothetical exercises. For example, we are also stress testing our capabilities with simulated attacks in the information security space.

These are just a few examples of the areas that the Business Resilience team is working on. Ultimately, our goal is to turn these initiatives into the normal course of how we think about risk and conduct our business in all parts of the firm to reinforce our commitment to resilience.

Challenges and Opportunities

Having covered the importance of an expanded remit for Risk, a systems view and the imperative to build resilience, let me discuss key challenges and opportunities for the industry to fully achieve these objectives. I don't have time to go through an exhaustive list, but I want to briefly describe three areas: 1) managing information, 2) rethinking models, and 3) industry cooperation and collaboration.

Managing Information: The Data Challenge

Let's begin with the challenge of managing information in the age of Big Data. The ecosystem of complex interconnections and multiple interdependencies among firms requires the collection, aggregation and analysis of massive amounts of data to paint a comprehensive view of systemic risk. As an industry, we have become very proficient at collecting reams of data, especially most recently in the OTC derivatives space, and we have also made progress in developing data standards and taxonomies, such as Legal Entity Identifiers – where SIFMA has been a strong supporter – that will allow us to aggregate data in a meaningful way.

But an even bigger question is, do we really know how to manage and interpret all this data? We believe we are still in need of more sophisticated analytical tools and data scientists to help us mine the data for actionable intelligence to identify risk trends, including potential extreme but plausible events that could spark contagion or create systemic shocks.

Rethinking Models

Analyzing data and information is one thing, but interpreting the data and understanding the implications for exposures based on our models for the financial system is another. We have all seen incidents that were once deemed unthinkable. Given the nature of complex adaptive systems, we need to reevaluate and supplement the tools we have traditionally used in Risk Management that have been based on assumptions of normal distributions and linear behavior, including the ability to capture interconnectedness.

In fact, we are already seeing some work progressing in this area. For example, the Office of Financial Research recently suggested using tools from process systems engineering to tackle the difficulties in identifying, modeling and analyzing data in the financial system. In addition, we have seen some work in Resilience Engineering, where techniques used to analyze safety, something called Functional Resonance Analysis Modeling (FRAM), is being used to analyze financial systems.

Industry Cooperation & Collaboration

If we take a systems-oriented view of risk, recognizing the interconnectedness of institutions and building resilience will require (1) information-sharing and (2) collaboration across geographic boundaries, particularly between market infrastructures, our users and regulators who increasingly have access to important data that can help complete the full picture of a bank's interdependencies.

One example of where DTCC has done work to improve information sharing is our initiative with The Financial Services Information Sharing and Analysis Center (FS-ISAC) to create a new joint venture, Soltra, which is developing and rolling out tools for automating the sharing of threat information within financial services as well as other industries.

Joint Industry Exercises

Another important area of collaboration is joint industry exercises. I mentioned earlier the work we are doing in scenario analysis and I know many other firms are doing the same. However, given the interconnections among our institutions, scenario exercises could be even more powerful if done jointly across the industry. For example, industry exercises like SIFMA's Quantum Dawn allow us to rehearse our response and adaptability to crises. The good news is that we are seeing significant collaboration in the industry today and this will pay long-term dividends in terms of building industry resilience and protecting market stability in light of some of the initiatives I mentioned previously and other projects, such as the shortening of the U.S. settlement cycle.

Conclusion

So in conclusion, allow me to summarize the key points I wanted to share:

The complexity of the financial ecosystem demands that we rethink our approach to risk management, which includes expanding the view of the various risks we need to manage and growing the remit of the risk management function.

We also need to move from linear ways of thinking to a more systems-oriented approach to give us the flexibility and agility to respond to tail events. We can do this by expanding the boundaries in which we view risks and shifting the time horizon forward to think about the unthinkable, rather than just looking at the past.

Given the openness and complexity of the financial ecosystem, it is inevitable that there will be breakdowns, so we also need to be prepared to recover quickly and think not just about managing risk but also building resilience. This commitment to resilience requires a corporate culture that fosters a learning mindset and that empowers all employees to become risk managers.

And finally, we discussed some of the key challenges and opportunities ahead, including our need to grow our skills at managing information in the era of Big Data, rethinking long-standing assumptions around risk models and fostering greater cooperation and collaboration among the industry.

The industry has made tremendous progress in expanding and improving the risk management function in recent years, but there is still much work to do to ensure we are prepared to protect against the many new risks the industry faces. If our industry becomes the leader in managing risks for our interconnected global system and for our clients, including ultimate end investors, that will be a key factor in increasing confidence in our industry and enabling future growth. We look forward to working with all of you on this in the years ahead.

I want to again thank SIFMA for the opportunity to talk to you this morning. I am happy to take any questions you may have.