DTCC Risk Forum

By Michael Bodson, DTCC President and CEO

Mike Bodson Opening Remarks
November 15, 2016

Resilience and Transparency

Welcome

Good morning, thank you all for joining us today. I also want to thank our Risk team for organizing this event and bringing together risk managers from across the industry to discuss the critical issues that we're facing right now.

DTCC Group Chief Risk Officer Andrew Gray spoke briefly about the evolution and expansion of risk management and, more generally, how systemic risks are becoming more severe, unpredictable and frequent. I want to pick up on this thought as it will underpin much of the discussion we have today.

Because risk is an inherent part of financial markets, financial firms need to become more resilient to protect against an ever-growing list of systemic threats.

But what do we mean by that?

Resilience isn't simply about the ability of a firm to return to its original state after a shock. Rather, because we take a holistic view of risk, we know that in a complex and interconnected environment resilience needs to be evolutionary and adaptable.

Resilience allows us the capacity to grow beyond where we were at the time of a shock, and to adjust our actions going forward based on the lessons of our experience.

There are many building blocks to increasing resiliency, but one of the most critical is transparency. I'm reminded of a famous quote from Warren Buffett: "You only find out who is swimming naked when the tide goes out."

Buffett is right about that, but the problem is that we can't wait for the tide of the next crisis to see who is naked, or at least unprepared. As a result, we need to increase transparency to better guard against risk, to better withstand future shocks, and to be better prepared to adapt and learn from them in the future.

That is why we're here today.

Key Topics

With that as a backdrop, I'd like to briefly focus on three points related to the current landscape of financial services and offer some thoughts on our path forward:

- **One,** I want to highlight several emerging risks and industry risk trends…
- **Two,** I want to discuss industry and regulatory responses to these risk trends, and…
- **Three,** I want to explain how transparency can strengthen resiliency to help create a stronger financial system.

Point #1: Current Risk Trends Impacting Finance

Let me begin with my first point on emerging risks and risk trends by touching on key highlights from the new DTCC Systemic Risk Barometer, which we released just last week. This is a bi-annual poll we conduct of risk managers globally to gain insight into the top risk issues impacting you and your firms as well as concerns you have about the future.

Not surprisingly, cyber risk was again the top concern in the survey, which would be expected given the uptick in high-profile attacks we've seen recently. I'll talk about cyber in a few minutes, but right now I want to focus on the other risks in the Top 5 because they are all related and paint an interesting picture that bears discussion.

Geopolitical Risks

In order of priority, the top risks were the results of the U.S. Presidential Election, geopolitical risk, the impact of new regulations and Brexit. While these risks are all very different, we can bucket them into a single category of geopolitical risk. And what they tell us is that there is genuine concern over uncertainty around the actions of government and their potential impact on our businesses.

The U.S. election saw anti-Wall Street rhetoric from both major candidates, and now that Donald Trump has won, we are waiting to see whether he acts on that rhetoric and who fills key positions in his administration.

While the results of the election could be seen as surprising, especially to pollsters and other so-called experts, what was even more shocking was the market reaction—which in many ways was the exact opposite of most analysts' predictions.

There's a lesson we need to take from this: As financial institutions, we must be ready not only for the unexpected, but we also have to be prepared for impacts that are the polar opposite of what you assumed would happen.

Brexit

This is, in some ways, similar to the Brexit vote in June. Both issues will have a bearing on the regulatory impact on the industry.

Nearly every firm represented here today has operations in the U.K., and the vote to leave the EU has created many questions about the future of those operations. And now there is even uncertainty whether the referendum is binding. While there is a lot more to come on these issues, what is clear is the level of uncertainty this is causing banks and their clients – the investing public.

DTCC Managing Director Mark Wetjen and Secretary Marcel Lettre of the U.S. Defense Departmant, and then Sonja Gibbs of the Institute for International Finance, will discuss geopolitical risks in a few minutes—and I want to thank both of them for joining us today.

Cyber Risk

Let me now return to cyber security for a moment. The real shocker of our Risk Barometer would have been had this issue not ranked #1 considering how WikiLeaks shaped the final month of the U.S. Presidential election and the high-profile Distributed Denial of Service attack in October that impacted some of the world's most popular websites, including Twitter, PayPal and Netflix. And, of course, we're all well aware of the attack on the SWIFT network this past spring that resulted in the theft of $81 million from the central bank of Bangladesh.

While geopolitical risks tend to ebb and flow over time, cyber risks continue to increase – and the risk to information security by those who exploit vulnerabilities in technology have the potential to be devastating to a single firm or, to be blunt, the entire global financial system.

It's no wonder, then, that firms are dedicating increasing resources to combat cyber attacks. While this is important to build stronger defenses, even more critical is that firms treat cyber risk similarly to all the other risks we face – that is, as part of a holistic view of risk management. We'll talk more about this over the course of today's conference.

Point #2: Industry & Regulatory Responses

Let me continue talking about the issue of cyber security as I turn to my second topic – how the industry and regulators are responding to these risks.

Over most of the past decade, we've seen a running battle of measures and countermeasures as corporations attempt to fight back against cyber attackers, who have become increasing sophisticated and more dangerous over time.

While a robust set of internal controls has been a critical component of a cyber security strategy, current complexities no longer allow firms to attempt to independently protect themselves against the myriad of existing threats. As with other facets of risk management, taking a holistic view that looks beyond a firm's four walls holds the promise of greater resilience.

Therefore, perhaps the single most important development in recent years has been the growing acceptance of collaboration among the industry and with regulators.

Hamilton Exercises

For example, cooperative efforts, such as the Hamilton Exercises and Quantum Dawn, enable financial institutions and the sector as a whole to practice and improve coordination with key industry and government partners in order to maintain market operations in the event of a systemic cyber attack.

These exercises allow the industry to work together to provide system-wide safeguards to limit wide-spread impacts in the event of a successful attack.

In fact, cyber risk has become so significant that many people have begun to question how long it will be before investors, clients and other stakeholders will require financial institutions to provide some form of independent attestation – similar to Sarbanes-Oxley or financial audited statements – that they have in place adequate cyber security measures related to themselves, their suppliers and other parts of the ecosystem.

This is understandable given the threat environment, but it has the potential to become overwhelming if there is not a pragmatic, collaborative approach and process to avoid multiple bilateral uncoordinated information requests or attestations. It's still early days on this issue, but it's something we need to keep in mind and get in front of.

Harmonization of Regulations

In that same regard, as the cyber threat has grown, regulatory agencies are seeking to gain a better understanding of the challenges we face, and today we see multiple regulators across jurisdictions issuing new mandates—something that one of our panels will discuss in more detail a little later…

Most recently, the Fed, FDIC, and OCC released a request for comment about proposed rulemaking on enhancing cyber risk management standards.

While that request acknowledges other regulatory requirements and guidelines—from the U.S. and globally via CPMI-IOSCO—it raises an important issue for the industry that needs to be addressed promptly: that is, the seemingly limited effort globally to harmonize proposals across jurisdictions.

This is problematic for a couple of key reasons. First, it raises the risk that multiple and uncoordinated regulations could divert attention and resources from dealing with cyber defense. Second, it creates compliance risk for firms that operate in more than one region by requiring them to adhere to potentially duplicative or contradictory regulatory regimes.

This is a common problem we face on a wide range of issues that extend beyond cyber security. We've seen it with new clearing mandates, capital requirements, and reporting rules.

In too many cases, policymakers are developing regulations for their home markets, but they need to also work collaboratively with their colleagues across the world to develop a common set of principal-based rules for firms to follow.

Certainly, all regulators share the goal of greater transparency to understand the cyber threats and their potential impact on the industry. But uncoordinated transparency mandates can sap resources that detract from building resiliency.

Point #3: Resilience and Transparency

And that brings me to my third point, how transparency strengthens resiliency.

By resilience, we need to do more than just measure, analyze and mitigate risk. Because the environment today makes a breakdown inevitable, firms need to be able to detect problems earlier and recover as efficiently as possible while minimizing contagion, and ultimately learning from these events to be better prepared in the future.

Every element of making a firm more resilient—from measuring, analyzing and mitigating risk to detecting, recovering and learning from an event—can be improved by increasing transparency to gain access to more information and a better view of the environment.

Therefore, transparency is also crucial for taking a systems view of risk, which requires looking at risk beyond one's own institution and understanding the connections between your own firm and others, as well as understanding how risk might propagate across those interconnections.

Because the weakest link can potentially bring down the whole system, transparency is a critical tool that can help identify that weak link. Common to all of these efforts is collaboration.

Collaboration among industry participants, and between the industry and regulators, is crucial to ensure the greatest possible harmony in achieving the shared goal of increased resilience.

Conclusion

As I close, I want to reinforce that collaboration requires constant dialogue among peers, and with clients.

This dialogue allows us to identify the key risks we share, whether cyber security or geopolitical, market or operational risks.

So let's continue this dialogue today to increase transparency and build a more resilient industry going forward.

I want to thank you again for joining us today.