Sarah Dahlgren: The importance of addressing cybersecurity risks in the financial sector

Remarks by Ms Sarah Dahlgren, Executive Vice President of the Financial Institution Supervision Group of the Federal Reserve Bank of New York, at the OpRisk North America Annual Conference, New York City, 24 March 2015.

* * *

Introduction

I would like to thank Operational Risk & Regulation for inviting me to speak here today. I appreciate the opportunity to address this group and kick off what looks like a very interesting and comprehensive few days of dialogue around current and future risks facing the industry.

As always, my remarks today reflect my own views and not necessarily those of the Federal Reserve Bank of New York or the Federal Reserve System.

I will begin my remarks with a high-level overview of the progress made in recent years in addressing some of the most significant risks facing the industry following the financial crisis.

I will then go on to discuss one of the areas where I see some of the biggest challenges in the road ahead. As the industry continues to adapt to and implement necessary regulatory changes, it is also adapting to and leveraging technology changes: technology changes that offer both exciting opportunities and more complex risks than – I think – we are prepared for.

Progress

Coming out of the financial crisis, we all knew that we needed to be better prepared for future crisis events, whatever their character, source or timing. We needed financial firms, and a financial system, that was better prepared to weather all storms.

In 2011, we developed the Framework for Supervision – a framework designed to ensure we had firms and a system that were less complex, more resilient and better managed.

Collectively, we have made a lot of progress since 2011 – and the industry is in much better condition relative to the pre-crisis period. But, as you all know, business does not stand still and this constant evolution results in new risks and new challenges.

Before turning to one of the biggest risks or challenges I see, I want to pause and recognize two things:

- First, it's clear that progress has been made across the industry in a number of areas – particularly in making firms and the system more resilient through improvements in capital and liquidity, as well as enhancements in risk management, including capital planning and stress testing across the range of risks firms face. But, in the remaining two areas of the Framework – less complex and better managed – I think it's safe to say that despite the fact that firms are addressing a number of outstanding issues, these areas continue to present challenges in reaching the desired end state.
- Second, as I'm sure you would agree, we collectively still have quite a bit of work to do to fully implement all of the changes required under new rules and regulations. And, we must continue to devote sufficient attention and resources to complete the efforts. At the same time, though, it is important to take stock of the changes made over the past few years – for two important reasons: first, to assess the impact of those changes, both intended and unintended; and, second, to understand the contours of the "new" financial system operating under the range of new rules and regulations, both national and global in nature. Such a stocktaking is important to

ensure that we collectively understand how the "new" financial system is operating. Firms and supervisors will continue to face challenges and competing demands as we press, in the months and years ahead, on implementing necessary changes and assessing the "new" financial system.

What the future holds

One of the topics that I feel will compete for, and will deserve, a lot of attention in the foreseeable future is cybersecurity.

I am often asked about my list of "things that keep me awake at night," and I think it's fair to say that cybersecurity is at the top of that list – as I'm sure it is for many of you in this room.

In fact, I think cybersecurity is one of the topics that should be on everyone's list – from the most senior managers and boards of directors, all the way down to line managers. Cybersecurity is not a topic or an issue just for the Information Technology staff or the CIO to address; it is a risk that isn't exclusive in who, what or where it targets.

- It is a risk that is difficult to clearly define.
- It is a risk that is constantly evolving.
- It is a risk that is not limited to one source.
- It is a risk that is faced by every single financial firm, regardless of size or complexity.
- In fact, it is a risk that is faced by every business, organization, school, church or group that uses technology. In other words, no company is immune (unless, of course, you operate an all cash business from a brick and mortar store and keep your earnings under your mattress – not something we see a lot of in today's world).

The financial sector, in particular, is under unprecedented attack from a broad spectrum of intent and attack methods that are complex, widely distributed, and increasingly interconnected. These highly dynamic systems give rise to the "new normal" – system design and architecture that needs to support rapid and compartmentalized change.

So, where do we begin when we look at a risk of this magnitude? And, how do we get our arms around the many associated risks that surround it?

Let me begin with what it is not. Cybersecurity is not an "Information Technology" issue. It is not a risk that can be addressed by simply having a strong IT team in place. It is not a risk that just affects a firm's technology – it affects the business itself, in every aspect – the bottom line, reputation, processes, and so much more.

However, information technology and cybersecurity are intrinsically linked. I'd like to cover both of these issues in my remaining remarks and focus on several of the underlying issues that need to be addressed.

Information technology and legacy issues

The first dimension is legacy: there is still a great deal of "clean-up" to do to fix longstanding technology and data issues that have built up over the years. The investments necessary are long-term and the fixes, in many cases, will take multiple years to execute. The range of issues include: systems or processes that are manual or not fully automated; asset management tools that are drastically insufficient; and business processes and models built without security requirements, to name but a few.

As firms address these challenges, they must also be flexible and agile enough to keep up with the changing environment and incorporate new developments as they arise. While a number of firms have sound programs in place to address these longstanding issues, strong

project management and tenacity will be crucial to see them through. In addition, continued prioritization and commitment of resources, as well as support from the firm's senior management and board of directors, are critical. I see commitment to this basic "blocking and tackling" as essential to financial institutions' continuing to be competitive – and relevant – in the digital world.

While the legacy issues need to be addressed in the near-term and quickly, we can't hold off on addressing the vast number of issues around cyber – since cyber is upon us now.

Information technology and cybersecurity

The area where I will spend most of my time discussing today is cybersecurity. Suffice it to say that as I think about the kinds of risks that might cause the next crisis, cybersecurity is the one that worries me the most. While I will focus my remarks on the financial sector, my concern is not limited to the financial sector. This is much bigger than just banks or financial institutions; it includes many other sectors as well.

As it relates to the financial industry in particular, the interconnectedness of firms continues to pose a particular risk to financial stability; from trading systems to settlement activities, we are at risk of a major disruption to financial stability. During the last financial crisis, we began to get a glimpse into the challenges faced as a result of interconnectedness and systemic failures. Years later, we are still faced with some of the same challenges, with only a limited view into the true complexities behind how firms are linked, connected, and ultimately intertwined to form the fabric of the financial industry. While we have begun to address other areas of systemic risk, I feel the industry as a whole is just beginning to scratch the surface of the potential system-wide impact of a significant cyber-attack. This risk can be referred to as "single point of failure." What is this? These are areas that, despite all of the work that has already been carried out, are significantly more vulnerable than others. We need to identify where they are and focus our combined efforts on understanding their systemic impact and addressing them.

I want to be very clear here. I don't think that this isn't a regular topic of conversation among directors, executives and managers – in fact, based on discussions I've had with many of you, I know that it's quite the opposite. There is a lot of discussion within firms about the topic – and there's quite a bit of activity more broadly that suggests that many different people are talking about cyber. There are conferences on cybersecurity every week. Consultancy firms are working with the industry on how to protect against attacks. Law enforcement agencies are investigating and cracking down on attacks and those behind them. Everyone is talking about this! And, I think that's appropriate and necessary – this is everyone's issue.

As we engage in discussions on the subject and flesh out our plans to address this risk, there are a number of topics that are key to keep in mind. Before I go through that list, I want to provide an overview on where we, at the Federal Reserve Bank of New York, are in our process.

While cybersecurity has been on our agenda for quite some time, and we have been dedicating resources to assessing it in large complex firms and setting expectations for smaller firms, we have elevated our efforts in recent months and have formed a dedicated team focused on further strengthening our overall supervisory approach to cybersecurity. As I mentioned at the beginning, I think we've done a reasonable job in developing rules and regulations to ensure firms are prepared to withstand the other types of shocks we have experienced in the past. But, cyber adds an element to planning for the next crisis that goes beyond what additional capital and liquidity, for example, can provide to the system.

The newly-formed team, led by Roy Thetford, the former Information Security Officer for the Bank, will be working with our examination teams to establish a new risk-based cybersecurity assessment framework, based on best practices in the field, as well as exploring additional standards that might be set out for supervised institutions.

In addition, to further strengthen and build out our program, we will be collaborating with critical stakeholders, including experts in security and cybersecurity; financial institutions, including both banks and non-banks; critical third-party service providers; domestic regulatory bodies; enforcement agencies; and international supervisors. As we move forward with developing the framework and standards, we are reviewing current and emerging laws, regulations and guidance; further researching best practices; and identifying gaps in current assessment efforts. As we do this, we have identified a set of issues that are top of mind:

1. This is not just an IT issue

As I mentioned earlier, cyber isn't just an IT issue. I don't think I can say this enough. It is a business issue first and foremost and needs to be tackled as such. Cyber needs to be owned by the business leaders in the firm – partnering with the experts of course. There needs to be a foundational shift in thinking at the top of the house: it needs to be a regular topic on the agenda for the board of directors; it needs to be at the top of the priority list for senior management of the firm; and it needs to be on the mind of every employee, to some extent. It needs to be part of everyone's vocabulary and recognized as a valid threat at every level.

2. Good risk management is the foundation

Good risk management and good IT practices set the foundation for a solid program to address cyber-related risk. It's hard to imagine that a firm that doesn't manage its IT risk well is ever going to be able to manage cyber risk well. In fact, two areas that we recently reviewed that require attention include basic IT asset management and strengthening patch and vulnerability management practices. These are necessary hygiene steps and should be a fundamental for a sound cyber security defense program.

As part of good risk management, firms also need to start considering how to assess the costs of cyber and connect the pricing of cyber risk to the businesses. You must ask yourself "what is my cyber exposure?" And, you need to think about how you should price it, because until cyber is priced, it may not get the attention it needs.

3. It's not just the banks

Cyber isn't just about the banks – it's about the entire financial sector, as well as the connections between the financial sector and other sectors like the utilities, retail, and others. We know that every area of the industry is interconnected; and it's not just financial firms. As the old saying goes, we are only as strong as the weakest link. In the financial system, that weak link could be a weak firm, a weak vendor, a weak point of vulnerability in a payments or clearing system, etc. A weakness in any of these areas exposes the entire system, because the interconnections mean that you are all linked to each other, to non-financial firms, and to every system that supports the operations and structure of the industry. The additional risk to keep in mind here is the growing number of unregulated firms operating in and competing in this arena. As the industry moves to overcome the risks associated with cybersecurity, you have to consider the additional vulnerabilities you are exposed to through non-regulated entities that will not be subject to the same guidance and standards. The big question lies in how you, as an industry, ensure that the 'industry as a whole' is safe, not just regulated entities.

4. One size does not fit all

Just as firms are diverse in size, complexity and product offerings, so too are technologies, processes and systems. While some firms house all technology work internally, others outsource the entire function or a significant part of it to third-party vendors.

In addition to the variety of systems used and approaches to information security within firms, as I said earlier, we have an entire subsystem that supports the financial sector and ultimately connects every firm to some extent. In response to this, we are working under the

assumption that there will not be a one-size-fits-all solution and the approach taken will need to be comprehensive and flexible enough to be adopted by all types of firms.

5. We are in this together

Cybersecurity is an area where I believe our interests are aligned and our shared goal is two-fold. In addition to wanting to see firms that are adequately protected against cyber-attacks and prepared to respond should they occur, we are equally as concerned with the overall safety and soundness of the financial system – as a whole. No one firm or agency is going to come up with the one and only permanent solution or protection against cyber-attacks. I see how we approach cybersecurity similar to how we approached Y2K – I'm sure you all remember that.

- We need an approach that everyone agrees to adopt.
- We need to see more public/private partnerships in the development of that approach.
- We need to come together to identify the vulnerabilities that are shared and what needs to be done.
- We need to agree on a path forward and how we test it.
- We need to acknowledge that, unlike Y2K, this does not have an expiration date.

Cybersecurity is a "new normal." It is going to become part of our vocabulary in nearly every exam we conduct, conversation we have with senior management, and conversation about the future of financial services.

To be successful, we have to agree that we have common goals; although we can approach them from different angles and think creatively about solutions, we should all be working toward understanding the threats we are facing. The threat landscape is shifting constantly, and we are all responsible for keeping up with the changes and adapting our controls accordingly. This includes firms, systems that support the industry, third party vendors, consultants, regulators, and law enforcement.

6. We need to leverage best practices

Leveraging a common set of best practices across the industry will be an important first step in closing the gap on the current vulnerabilities. Unlike the approaches taken by other supervisors to address cybersecurity concerns, our initial focus in this area is on better understanding the vulnerabilities, how firms are addressing them, what progress has been made by firms and assessing where the industry stands as a whole. Yes, we want you to address the weaknesses, but this is a lot bigger than the weaknesses identified at one firm.

We will be looking to firms to leverage guidance around best practices to identify their weaknesses, and we want firms to bring forward other issues, concerns or vulnerabilities they encounter in doing so. We need to identify, as an industry, where the risks truly lie and what we are doing about them.

There has been a lot of work done in this area by experts, including the NIST, the FBIIC, FINRA, PRA, FFIEC, NCUA, etc. – the list goes on. And, there are a number of sets of best practices already published. We are aware that firms have been looking for guidance on which approach to take or framework to adopt. As we review all published guidance, assess the broad volume of research that is already out there and come to consensus on an evaluation framework, we encourage firms to look at the fundamental commonalities across all best practices and build them into your ongoing/current activities.

7. Assessing the threat

To fully assess a threat or risk to a firm, we must first understand where the risk lies, who it affects, how it is defined, and what the associated costs are. In the case of assessing the risk and impact of cyber-attacks, I believe firms need to be cognizant that every business decision, every process, every change a firm makes ultimately has a cyber-related element to it. To add to the complexity of this, the firm's self-awareness must extend beyond the four walls of their company and must also take into account the impact critical service providers have on the firm. You can outsource the service, but not the risk.

Everyone should be using threat intelligence as we go about our day-to-day activities – using the potential of a cyber-attack as another filter through which we view every decision. As we think about the variables to be considered in the decision-making process, we must build in the potential for creating weaknesses, vulnerabilities or opportunities for cyber-attacks, and be aware of the associated costs.

I fear that until we can assign financial consequences to cyber risks, and ensure staff are taking that into account when making decisions, we will not get the commitment needed from every level of the organization to adequately address the problem. As long as decisions are made and actions are taken without this type of assessment, we are going to see more and more of these weaknesses exposed. These vulnerabilities are not necessarily new, but the exposure to them is increasingly being made available to attackers. For instance, a weak patch management process comes with the risk that systems may take longer to patch (or not be patched at all!) resulting in a much larger target window of opportunity for attackers.

As we assess the potential impact, it is also important to remember that protecting against an attack is only half the solution – particularly because, as my InfoSec colleagues like to say: "It's not a matter of IF we get hacked; it's a matter of WHEN." A strong cyber resiliency program is a good starting point to address this, but we also need to focus on limiting the impact following an attack by addressing the fundamental structure within the organization – how safe is the system, how compartmentalized are the core areas of technology, and what your ability is to isolate the threat.

8. Need to address communications

Finally, to successfully address this risk with a unified front, we must develop an approach to enhanced communications around cyber threats and events, and revisit supervisory guidance in this area. Silence and fear of sharing intelligence in this area could be detrimental to efforts to address the vulnerabilities systematically. We know that breaches have occurred and will continue to occur until the industry is better equipped to be ahead of the attackers, not playing catch up. Right now we are interested in learning from these breaches and using intelligence garnered to get ahead of game.

There is a lot to think about here. With all this in mind, I will end this part of my remarks with a reminder of what we see as the key components of any solution designed to address cybersecurity. It must:

- Be comprehensive, risk-based and threat-informed;
- Be a joint effort between public and private sectors;
- Be flexible enough to evolve as technology advances;
  - Automated
  - Scalable
- Support information sharing;
- Leverage best practices;

- Include all in the industry – regardless of size or processes (internal systems or external providers); and
- Delve deeper than one step below the surface.

Conclusion

We live in an ever-changing environment where speed and agility are of the essence. Demands from customers change, expectations from shareholders fluctuate and the regulatory landscape you work within will continue to evolve to keep pace. Constant change – and commitment to evolution – is not a choice. It is the only way to survive, stay competitive and stay safe in a complex and vulnerable world.

As it relates to cybersecurity, I believe we are at a pivotal moment: we know there is an issue; we will work with you on fully understanding the scope and breadth of the risk; we will be pragmatic and add value; we are looking at this holistically; and our goal is to come out with a set of next steps that will benefit all of us, including protecting the financial system and the U.S. economy as a whole.

We need to address cybersecurity before we see a catastrophic event, not analyze it afterwards.

Thank you.