U.S. DEPARTMENT OF THE TREASURY

Press Center

Assistant Secretary Amias Gerety Remarks before the 24th World Congress of Savings and Retail Banks

9/24/2015

Introduction

Thank you for the opportunity to speak with you today. I'm pleased to be able to join what I'm told has been a robust discussion about the digitalization of the global economy and its impact on our individual communities. I think all of us would agree that our increasing interconnectedness is an incredible and perhaps unprecedented opportunity for positive change around the world that has already improved the quality of life for millions. This change does of course carry with it some risk, and I would like to spend my time with you today discussing one risk in particular, namely the threat posed by malicious cyber activity targeting our financial system, including toward small and medium sized banks.

It seems that each week brings a new report of a cybersecurity attack against a U.S. business. And this is not limited to large companies. Many of you have likely managed the response to a cyber-incident yourselves. Even if your bank has not been directly impacted, credit and debit card information is targeted every day, and your staff should be prepared to answer customers' questions and help them understand the risks they face.

Unfortunately, the cybersecurity challenges we are confronting extend even beyond stolen credit card data and identity theft. Malicious cyber actors come in many forms and have diverse motives. Some actors are intent on advancing a political agenda. Others steal intellectual property for economic gain. Perhaps most alarmingly, some malicious cyber actors seek to critically harm the U.S. through disruption or destruction of our most vital infrastructures, and this includes the financial sector.

When people think of the financial sector in the context of headline generating data breaches or threats to national, economic, and homeland security, they sometimes think only of attacks against major banks, financial markets, or financial utilities. However, the risk is more significant than that, and understanding how to effectively manage cybersecurity risk is a critical component to running any business today. This is, of course, not only true for the U.S., but also for the global financial community as a whole and especially for smaller firms, which are critical to the U.S. and global financial system. In addition, these firms often possess the attributes – stores of sensitive financial information, interconnectivity with other organizations, and a reliance on electronic systems, for instance – that make all financial institutions targets of malicious cyber actors. At the same time, we recognize that smaller companies often have fewer resources to manage what can be a highly technical and complex challenge, at least on its face.

For these reasons, the U.S. Department of the Treasury, along with our law enforcement, intelligence community, and homeland security partners, as well as financial regulators, is increasingly focused on how government can better support the cybersecurity needs of smaller financial institutions. We are doing so while continuing to grow our collaboration with the larger institutions we have been working with for some time.

Of course our efforts to assist smaller firms with this issue will only be successful if our programs reflect your priorities and are based on your feedback. With this in mind, I'd like to describe the Treasury's strategy for engaging with smaller firms on cybersecurity issues and to ask for you to join the discussions of these issues between government and the private sector at all levels in the U.S. and around the world.

Strategic Approach

We at the Treasury recognize that public-private collaboration is the corner stone of any effective strategy for reducing cybersecurity risk. The bulk of the critical systems we seek to secure and the architecture of the Internet that connects those systems together is owned and operated by private companies. This is fundamental to how we think about the Internet. This means that no single company, agency or sector possesses sufficient information to single-handedly manage our nation's cybersecurity risk. Instead, government and the private sector must work closely together in a collective effort. We have already seen this collaboration produce several significant positive steps, especially for the financial services sector, including:

- Improved actionable cybersecurity information sharing between government and industry, often through the Financial Services Information Sharing and Analysis Center (FS-ISAC);
- Development of the National Institute of Standards and Technology's Cybersecurity Framework, a voluntary tool that many organizations are using to effectively frame their approach to cybersecurity risk management. We've also recently seen our U.S. banking regulators collaborate on a Cyber Assessment Tool, which provides financial services sector institutions with a framework for assessing their cybersecurity risk posture; and
- Creation of stronger processes for responding to cybersecurity incidents that occur, especially those with the potential to have sector-wide impacts, which we've achieved in part through a recent series of cybersecurity exercises between government agencies and financial institutions.

While these efforts do not represent an easy way to solve our cybersecurity problems, they have been helpful and serve as a useful model for the sort of work Treasury and others in government should be doing with smaller institutions. At the same time, we also recognize that there is not a one-size-fits-all solution and some of our activities need to be tailored to the unique needs of smaller firms. With this in mind, we're developing a series of smaller firm specific initiatives that focus on the areas of information sharing, baseline protections, and incident response that I'd like to discuss with you in detail.

Information Sharing

Information sharing represents one of the most important ways of reducing overall cybersecurity risk. This sharing takes a few different forms but often involves the exchange of descriptive information about cybersecurity threats that business owners can use to better understand and prevent malicious cyber activity. Cybersecurity information sometimes comes from government, and Treasury has established the Financial Sector Cyber Intelligence Group to help identify information government possesses that may be useful to firms and to share that in a timely and actionable fashion with companies. In addition, FBI and DHS have also recently undertaken significant efforts to expand their information sharing activities. The government, however, certainly does not have a monopoly on useful cybersecurity information.

The private sector also possesses a tremendous amount of cyber data, and many financial services sector companies are on the cutting edge of sharing these types of information among themselves and with government. Much of this sharing is facilitated by the FS-ISAC, which includes government agencies, banks, insurance companies, broker-dealers, exchanges, other financial institutions, and companies that support worldwide financial services sector members.

I hope many of you are already participating in the FS-ISAC's work. Even so, we believe it critical that more firms participate, especially smaller institutions. Progress has recently been made in promoting this goal with an agreement between the U.S. Federal Reserve Banks and the FS-ISAC to provide access to security threat information to the banks' financial institution customers.

In addition to exploring ways to involve smaller firms more directly in cybersecurity information sharing activities, we are also working to engage more directly with third-party service providers. These companies provide critical services to financial institutions, and are for some smaller firms the sole source of technological expertise and capability. For this reason, we view these service providers as "force multipliers" who can leverage the cybersecurity information they receive to help protect a diverse and broad set of firms.

Baseline Protections

Of course information sharing alone is not enough, and we must all take specific steps to improve our overall cybersecurity controls to build more secure networks. This work can be difficult, especially for firms will smaller technology staffs, and that's why we believe that the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework) can be very helpful to you. For those of you who don't know, this NIST Framework – which you can find online – is a voluntary tool for helping companies manage and reduce their cyber risk. By comparing your current cybersecurity activities to those outlined in the framework, you can improve your baseline security level and reduce the possible impact of an incident that may occur. The framework lays out a model for considering cyber risk based on five functions – identify, protect, detect, respond, and recover. Each function includes specific activities that you should consider pursuing as a part of your risk management program.

I want to emphasize that the NIST Framework is not just a tool for firms who manage their security in-house. Firms who contract for the bulk of their security and other services can apply the framework's methodology in discussions with service providers by asking them how their offerings align to your firm's particular risk model. Related to this, we're encouraged by the recent work of the Securities Industry and Financial Markets Association to create an auditable third-party risk and cybersecurity standard based in part on the NIST Framework.

To further encourage the NIST Framework's use, especially among smaller firms, Treasury is working to develop a set of cybersecurity "exercises in a box" aligned to key aspects of the framework. These exercises – which firms will be able to download from the Internet and use on their own – will enable boards of directors and senior management to assess their firms' cybersecurity risk management posture in the context of an exercise scenario.

Incident Response

The final area where we're focusing our engagement with smaller firms is on building stronger incident response processes both at the sector and firm-levels, especially processes for responding to cybersecurity incidents that have the potential to create sector-wide consequences. Even the most secure networks are still vulnerable and so it's important that we all have a shared understanding of what to do in the event of a crisis. Within firms, this means maintaining strong incident response plans that, for example, define roles and responsibilities for senior management as well as for technical experts. Another key component of any incident response plan is having a clearly identified process for coordinating with law enforcement, in addition to doing necessary reporting to financial regulators. As a part of this, it's critical that firms build strong relationship with law enforcement – and in the U.S. that often means the FBI and U.S. Secret Service – in advance of an incident occurring. These agencies can provide you with invaluable support. To aid in building connections between smaller firms and law enforcement, Treasury is joining forces with the FBI, the U.S. Secret Service, and the Financial Services Sector Coordinating Council to hold nationwide open house events that will welcome financial institutions to law enforcement field offices across the country to build and expand ties.

We're also working to involve smaller institutions in exercising national incident response processes. To do this, we're partnering with law enforcement and homeland security agencies, as well as financial regulators, to plan a series of regional cybersecurity exercises. These events, which will begin in early 2016, are an opportunity for firms to meet together with government agencies and walk through the response to a major cybersecurity incident. We plan to use these events not only to socialize response processes that are already in place, but also to collect additional feedback on how these processes can be improved.

Conclusion

I'd like to close by emphasizing that these activities alone are not enough, and that we need to find more ways to work together, especially across international borders. Cybersecurity has become a critical concern for many financial leaders around the world, which underscores the urgency of global coordination. As one example of how this cooperation can be done, the U.S. is currently working with our counterparts in the United Kingdom to plan a cybersecurity exercise focused on the financial services sector, which will in part be an opportunity for us to share approaches to managing cybersecurity risk.

We hope to do more such sharing of cybersecurity approaches in the future because cyber risk is an inherently international issue and a global concern, and we believe that the world can learn from our experience just as we can learn from yours. Many of our interdependencies rely on a well-functioning, reliable Internet, which can protect our information, and provide timely, secure and resilient service. We truly are all in this together.

I hope those of you who are visiting us from abroad will also consider the model I've described today as something that might work in your own countries, and that you will consider how we can best share other approaches to reducing cybersecurity risk.