U.S. DEPARTMENT OF THE TREASURY

Press Center

Remarks by Deputy Secretary Sarah Bloom Raskin at The Center For Strategic And International Studies Strategic Technologies Program

9/10/2015

As prepared for delivery

I. Introduction

Good morning. Thank you, Jim, for the introduction; and thank you to the Center for Strategic and International Studies for joining with the National Association of Insurance Commissioners to bring us today's event.

Four centuries ago, political philosophers developed a "social contract theory" to defend the legitimacy of government and explain its relationship to society and the people. These philosophers—people like Thomas Hobbes, John Locke, and Jean-Jacques Rousseau—all put a different spin on it, but the basic idea was that people traded their natural rights of vigilante self-defense and self-help for the protections offered by government with law enforcement and systems of civil and criminal justice. The theory was that all of our rights and property are safer if we consent to government than if we simply go it alone and remain in a state of nature, the place that Hobbes famously called "nasty, brutish, and short," and which too often comes to resemble a state of war.

In many parts of the world today—Syria comes quickly to mind—people are still struggling for the basic security and safety provided by civil government. The state of nature, as we see simply by opening up the morning newspaper, is still a state of war, chaos, theft, misery, and flight.

The world is also struggling to establish cyber protections because today, at least in the functioning civil societies, commerce, banking, culture, entertainment, insurance, payment systems, and government agencies are all on-line and interdependent.

We have seen how vulnerable all of our major economic and social sectors and institutions are to hacking and cyber-sabotage. The examples are well-known: Sony Pictures, JP Morgan Chase, Target, Anthem, the Office of Personnel Management. We know that cyber-terrorists would like to find a way to bring down all and anything that uses the Internet as an act of war against the network of civil societies that have created a new interconnected global community.

In the Internet Age, which is now beset with hacking, cyber-assaults, cyber-sabotage and cyber-warfare, an updated social contract is needed. What is the responsibility of government to protect us from cyber-enemies? What is the rightful expectation of private institutions, like insurance companies, banks, businesses and other organizations, to protect themselves—and to insure themselves—against cyber risk? How can private institutions best work with government to create strong cyber defenses? How do we defend the competing values of cybersecurity and Internet freedom? And while the new social contract is struggling to be born, what concretely should businesses, banks, insurance companies, and government officials be doing to protect all of us in the short-term?

These are not questions we can answer completely today, but the people assembled here are some of the best prepared to engage in this dialogue. The participants here today come with some of the best insights from the public sector and the private sector.

For the past 50 years, CSIS has been at the forefront in exploring the most vexing national security and foreign policy challenges facing our country and the world.

For its part, NAIC and its predecessors have served for almost 150 years as a forum for domestic insurance supervisors to set model standards and participate in insurance regulation and supervision nationally, and more recently, internationally.

Bringing both CSIS and NAIC together presents us with the opportunity to delve into the theme of one of our world's next great projects—namely the development of the arrangements among our society's participants in an inter-connected world, and the development, in the short term, of creating strong cyber defenses for our people. The missions of CSIS and NAIC create a natural nexus and opportunity because cyber risk affects both our national security and foreign policy interests, and also the United States' economic health and financial stability.

Your two organizations together are well equipped to help develop a common understanding of the cyber risks facing America, and how to best identify and mitigate those risks.

II. The Internet and Its Connections

So let's take a look at the risks.

The Internet, and the devices we use to access it, provide us with unprecedented linkage to one another and the world. By some estimates, this year 25 billion devices will be connected to the Internet, translating into more than three devices for each person on the planet.[1] And five years from now, in 2020, Internet-connected devices are expected to double, to 50 billion.[2]

As a mother of three young adults and teenagers, I'm convinced that most of these devices are in my household scattered like the shoes you trip over when you enter your front hall after a long day in the office, dropped here and there like Legos all the way to the dinner table, where they threaten to ring with catchy tunes.

In addition to personal computers and smart phones, today the Internet is connected to everything from our cars, parking meters, door locks, and thermostats to cardiac monitors, other medical devices, and even cows—yes cows so that farmers can monitor the location and health of their livestock remotely and in real-time.
What will tomorrow's connected devices include? We likely cannot imagine them all today.

Our economic activity is increasingly propelled through these devices; devices that present paths to the Internet's intricate web of connections but whose security has largely been an afterthought, until recently.

The Internet is where the American people communicate and engage in commerce. It is also where a vast amount of personal data is shared and accessible. The Internet is also where critical infrastructure organizations—energy, financial services, transportation, telecommunications, healthcare, and governments—do business.

We are so interconnected that the risk of contagion within and across our critical infrastructure creates potential national security and foreign policy concerns. It also creates concerns around our domestic economic health and financial stability.

III. The Threat

Not so long ago, cyber threats were largely tied to economic crimes and acts of vandalism by hackers or "hacktivists" with political or social agendas. But digital threats have now transcended economic and attention-seeking motives.

As you know, late last year, North Korea launched a destructive attack against Sony Pictures, destroying systems and wiping out data, along with the more sensational public posting of unreleased movies and confidential emails. An insidious geopolitical purpose was afoot: to damage, shame, and ultimately attempt to coerce a U.S. company and its personnel from exercising their right to free expression.

Less noticed, but also disturbing, was a cyberattack on a German steel mill last year. The attack began with so-called "spear phishing;" hackers sent targeted emails from seemingly trusted sources to trick plant personnel into opening attachments or visiting websites from which tainted software, or malware, was downloaded.[3]

That malware allowed hackers to steal computer login credentials from people who worked at the plant. Remotely working their way from the office into the production computer networks, hackers ultimately gained access to systems controlling the mill's manufacturing equipment.

Once the hackers got themselves inside the mill—possibly from the comfort of their living room sofas—they took control of the plant's systems. The plant's managers needed to shut down the blast furnace, but found that they could not; they no longer controlled the on-off switch, which had been appropriated and taken over by the hackers. In short, the plant was unable to control the shutdown of its furnace. And to think: It all began with an email.[4]
This certainly is a wakeup call.
Some of our nation's most prominent health insurers—Anthem, Premera, and CareFirst—were also targets of attacks this year.[5] The attackers stole the names, birthdates, and street and email addresses, and also, in some cases, took medical identification and social security numbers.[6]

In government, we are also not immune to the threat. This spring, we all know that the Office of Personnel Management announced a series of cybersecurity incidents and vulnerabilities that exposed sensitive personnel records and security-clearance files of 21.5 million current and former federal employees and contractors. The stolen records included detailed biographical information spanning from where people lived, worked, and were educated, to their relatives, friends, neighbors, and business associates, as well as sensitive health, criminal, and financial information.
The health insurance and OPM breaches are particularly alarming given the high black-market value placed on private health data as a tool for extortion, fraud, and identity theft. Personal information also can provide adversaries of the United States with information to target individuals for espionage or physical harm.

Indeed, in private companies and public institutions—and certainly across this administration and at the Department of the Treasury—cyber threats are recognized for what they are: One of the most pressing operational, financial stability, and national security risks of our time.

IV. The Response

So, how do we respond?

Given the growing frequency, sophistication, and morphing ability of cyberattacks, we—all levels of government, our critical infrastructure, our financial firms that contribute to our economic stability – including insurance – and frankly, all of us as individuals—have to take responsibility for protecting our nation, our individual and collective assets, and each other from cyber threats. As I see it, it's a collective responsibility. It's what I called it earlier—the updating of a social contract for the Internet Age.

A. The Role of Government

So first, let's talk about what governments can do. Governments can and do play an important role. In cyberspace, governments have unique capabilities that can be brought to bear to identify and counter threats, as well as mitigate harm.

A key responsibility for Treasury is helping to safeguard the resiliency of our economy and the financial sector, one part of which relates to cybersecurity and resiliency. We work closely with the Department of Homeland Security, financial regulators, including the NAIC, and the law enforcement and intelligence communities.

Our efforts include helping the financial sector increase baseline protections—like encouraging basic cyber defensiveness for financial institutions, and facilitating the sharing of cyber threat, vulnerability, and incident information.

We also help private institutions and other government agencies practice responding and recovering from simulated cyberattacks through a series of table-top exercises.

Treasury also works to deter illicit cyber activities and the individuals behind them both domestically and internationally. When traditional law enforcement and diplomatic engagement prove inadequate—and the exploits are significant and malicious—we can now impose targeted financial sanctions on individuals or entities overseas.

These sanctions are not intended for garden-variety malicious cyber activities. Instead, when cyber-enabled activities pose a threat to our national security, foreign policy, or economic health or financial stability, we now have the means to freeze assets, block transactions, and financially isolate the actors responsible for the most serious cyber threats facing our country.

In the current interconnected global environment, there is a growing consensus around the need to ensure that international legal principles pertain to state and non-state actors online just as they do offline. To improve cybersecurity around the world, we are working with the international community to develop common understandings of appropriate behavior in cyberspace.

B. The Role of the Insurance Sector

Next—beyond government—what about the insurance sector? The insurance sector plays a role in helping to quantify cyber risk.

For example, Lloyds and the University of Cambridge's Centre for Risk Studies recently published a study on the financial impact of a hypothetical cyberattack on the U.S. power grid.[7] Characterized as improbable but technologically possible—and eerily similar to the German mill attack I described earlier—the study highlights the potential systemic nature of cyber threats.

Using the Internet for initial access and later command and control, the scenario shows the potential cascading effect that a major attack could have, triggering monumental economic losses, in addition to losses from the direct damage to electricity plants and equipment. Economic costs included loss of revenue to affected plants and companies that distribute electricity. Costs also included losses to commerce, productivity, confidence, trade, and consumption.

Insurance companies know how to rigorously assess these kinds of losses. The insurance sector knows how to gauge the individual and collective risks and associated costs posed by cyber incidents.

Of course, insurers do more than just quantify risk; those that offer cyber risk insurance provide an important, monetary last-line of defense to their policyholders. Cyber insurance provides an important risk mitigation tool by allowing policyholders to transfer some financial exposure associated with cyber events.

Cyber insurance can play another role as well. The underwriting process itself can bolster cybersecurity. To qualify for cyber insurance, a business typically fills out an application seeking details on its risk level and controls that mitigate the risk. The act of engaging in this process helps businesses identify tools and best practices that they may be lacking.

Some insurers go a step further by asking questions during the underwriting process to better gauge how embedded cybersecurity is in a company's governance, control, and enterprise risk management infrastructures.

These insurers ask their customers: Is cybersecurity part of the company's risk management framework? Are third-party service providers evaluated to ensure their adherence to the company's cyber requirements? Does the company have a cyber-incident response plan, or a documented playbook to guide response from a significant cyber event?

Does the company engage in basic cyber hygiene necessary for good defensiveness, such as regular patching of software and scanning for malicious activity, and mandating multi-step identity checks—known as multi-factor authentication—to access company networks?

Just by asking these types of questions and making them part of the underwriting process, insurers can move the needle. When organizations embed cybersecurity into their core governance, control, and enterprise risk management infrastructures—when that cybersecurity is tailored to, and part and parcel of, systems, operations, and processes—multiple lines of defense are created.

When this happens, it is a game changer. Why? Instead of grafting cybersecurity controls on top of existing controls hoping they'll stick, cybersecurity becomes part of an organization's DNA. When done right, collective defenses—a combination of people, processes, and technology—cannot be circumvented, removed, or defeated.

Just as the insurance industry can assist businesses in mitigating their cyber risks, the industry can help us all by leading by example in managing its own cyber risk. Whether a large insurer operating in all 50 states and internationally, or a small mutual insurance company with a limited scope of business and geographic reach, insurers collect and store highly sensitive policyholder information. This data is a key asset which, if exposed, as we all know, may violate privacy laws, or certainly privacy expectations, and may lead to substantial consumer and reputational harm. Encrypting sensitive data throughout its lifecycle—both in transit and at rest—is one key control.

Insurance companies cannot stop at their own cybersecurity controls, either; they must also make sure that their third-party vendors have cybersecurity that is up to par. Insurance data is not just used by the insurers, but by a whole range of others that assist with actuarial, underwriting, and claims adjusting processes.

C. The Role of Insurance Regulators

I've spoken about the roles of Treasury and the federal government and the insurance industry. Now I'd like to close by briefly touching on the essential role of another vital part of government, the state insurance regulators.

In many ways state insurance regulators, many of whom are here today, are the cops on the beat when it comes to cybersecurity at insurance companies and the protection of sensitive information of applicants and policyholders. But state regulators need not go it alone.

I commend NAIC for recently appointing a task force to centralize insurance regulatory activities around cybersecurity. This past spring that task force adopted 12 principles for insurers and other regulated entities to join forces in identifying risks and adopting practical solutions to protect information entrusted to them.[8] NAIC has also developed guiding principles for insurers underwriting cyber risk and is developing a set of best practices for examiners to test insurers' processes and protocols around data protection and cybersecurity.[9]

Along with other state and federal financial regulators, NAIC is also a member of the Financial and Banking Information Infrastructure Committee[10]. Cybersecurity is on the top of this group's agenda.

Last summer I launched regular principal-level meetings of the committee. At these meetings we focus on strategic issues around cybersecurity. Topics range from removing information-sharing impediments and enhancing incident-response planning, to examining financial firms to identify best practices around cybersecurity controls. Adam Hamm—the Insurance Commissioner for the State of North Dakota and a speaker on today's second panel—has been an active and thoughtful participant.
International engagement is also essential. Treasury, through our Federal Insurance Office, and NAIC need to continue their collective work with the International Association of Insurance Supervisors, a key international standard-setting body for insurance. In the coming months, IAIS will be assessing whether to revise global standards and guidelines for insurance supervision to better address cybersecurity and related technology issues.

V. Conclusion

This is but a start. Cyber risk goes to the core of our nation's security, and we have glimpsed the dire consequences of successful hacks, and cyber assaults against our country's assets and values. Mitigating these consequences is part of the project at hand—the project of updating our understanding of the responsibilities of government, commerce, and the individual in our inter-connected society—a collective engagement in establishing cyber protections when so many values are at stake.

Fortunately, we are all engaged. That's why even though cyber risk and the challenges posed by cybersecurity can seem daunting or insurmountable, addressing these challenges is how we give birth to a social contract that addresses cyber protections. Stay engaged because your insights and experience will mold the contours of a more cyber secure and resilient world.

Thank you.

###

[1] Dave Evans, Cisco Internet Business Solutions Group (IBSG), *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*, 3 (Apr. 2011).
[2] *Id.*
[3] http://www.wired.com/2015/01/german-steel-mill-hack-destruction/
[4] *See, e.g.* Die Lage der IT-Sicherheit in Deutschland 2014, Bundesamt für Sicherheit in der Informationstechnik (BSI), Nov. 2014; Robert Lee, Michael J. Assante, & Tim Conway, German Steel Mill Cyber Attack, SANS Industry Control Systems, Dec. 30, 2014, https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf (including assessment of attack and translation of relevant text from BSI report); Hack Attack Causes 'massive damage' at Steel Works, BBC News, Dec. 22, 2014, available at http://www.bbc.com/news/technology-30575104; Kim Zetter, A Cyberattack has Caused Confirmed Physical Damage for the Second Time Ever, WIRED, Jan. 8, 2015, available at http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
[5] Anthem Inc., at http://www.anthemfacts.com; Premera BlueCross, at http://www.premeraupdate.com/; CareFirst BlueCross BlueShield, at http://www.carefirstanswers.com/.
[6] *Id.*
[7] Lloyd's and University of Cambridge Centre for Risk Studies, Business Blackout: The insurance implications of a cyber attack on the US power grid (May 2015).
[8] National Association of Insurance Providers, at http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.
[9] *Id.*
[10] This committee was formed by the President's Working Group on Financial Markets after the attacks on September 11, 2011