Today's Mobile Cybersecurity Information Sharing

CTIA
The Wireless Association®

Executive Summary:

Effective cybersecurity requires information-sharing practices that provide for the ready and rapid exchange of cybersecurity-related threats, countermeasures and recovery mechanisms in a collective context across private sector and government entities. For cybersecurity, the meaning of information sharing is highly specialized because the information shared is confidential and exchanged in a trusted setting, which means a protected legal and legislative environment set up exclusively for cybersecurity purposes.

The importance of cybersecurity information sharing cannot be overstated.

To respond to the growing hostile environment, the wireless industry must have access to the latest intelligence gathered by U.S. cybersecurity experts on emerging threats, and the latest innovations in responses and protections, if the nation's highly interconnected digital ecosystem is to stay sufficiently secure to maintain the trust of consumers.

The importance of cybersecurity information sharing cannot be overstated. It serves as the essential and critical shield in the ongoing struggle to protect mobile devices, laptops and wireless Internet-based services against cyberthreats.

While the mobile industry supports and participates in many public-private partnerships that provide venues for the exchange of threat-information, there are limitations that adversely affect the timeliness of information sharing and collaboration within the private sector. The National Institute of Standards and Technology (NIST) published the Framework for Improving Critical Infrastructure Cybersecurity[1] that supports information sharing as a *central* component of the risk principles both within organizations and among industry segments and government.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

To establish the foundation on which modern information sharing can take place, the wireless industry recommends that cybersecurity legislation affirmatively address the principles of protection described herein.

Introduction

The wireless communications industry is committed to doing its part around the clock, seven days a week, to keep U.S. networks and end users secure. Ensuring that industry and government security experts can share information about cyberthreats on an ongoing basis is vitally important to containing the growing variety of intrusions and attacks from criminals and hackers, whether state-sponsored actors or activists with their own agendas.

Today's mobile cybersecurity is supported by a wide array of public-private forums created over time as a result of threats (natural disasters and man-caused) to the integrity of U.S. infrastructure, including its communications networks and systems. Member companies of CTIA–The Wireless Association and its Cybersecurity Working Group and Privacy Working Group actively participate in these industry and government partnerships.

Cybersecurity threats, however, continue to spread from other parts of the world to the United States, making the task of information sharing more urgent than ever.

As Congress considers various legislative proposals to strengthen the nation's cybersecurity and privacy protections, policymakers will be asked to make decisions that will either improve or impede the industry's ability to effectively share information to combat these threats.

To help inform these deliberations, this white paper provides an overview of three critical points:

- First, why information sharing is so important, in particular within the private sector;
- Second, what it contributes to the nation's cybersecurity defenses;
- Third, and perhaps most important, the remedies needed to overcome current limitations to effective information sharing so that our wireless communications systems and networks can continue to be protected in the face of accelerating global threats.

Before we address these central points, it is important to have a common understanding of what information sharing means in the context of keeping our networks secure from cyberthreats.

Cybersecurity Information Sharing: A Definition

Most uses of the phrase *information sharing* relate to an open exchange of data, ideas and content among various organizations, people and technologies. As the Internet expanded, bringing us such developments as wide distributed networks, intranets, cross-platform compatibility, application porting and standardization of IP protocols, it has made possible growth in information sharing on a massive, previously undreamed of global scale.

However, in the realm of cybersecurity, the meaning of information sharing is highly specialized and complex. Because of concern that the data, or information, being shared could inadvertently expose personally identifiable information, proprietary, confidential or other protected data, or give the bad guys clues about discoveries of weaknesses in widely used software or interconnections, or the latest protections being deployed, cybersecurity information sharing can be generally described as follows:

> *The sharing of information in a confidential, trusted setting, which means a protected legal and legislative environment, exclusively for cybersecurity purposes. Cybersecurity purposes include: indicators of cyberthreats and attacks; monitoring of threats and application of countermeasures; and discussions and findings about development and testing of new defenses and standards, with the aim of preserving and strengthening security across communications networks and systems.*[2]

...in the realm of cybersecurity, the meaning of information sharing is highly specialized and complex.

Cybersecurity information sharing ***is:***

- Necessary to maintain the strong lines of confidential dialogue needed to ensure robust defense, recovery and response in an interconnected communications environment,

...it is important to recognize the distinction when considering the importance of information sharing...

- Essential to assessing threats to bolster the ability of government and industry to mitigate or recover quickly from cyber intrusions or attacks,
- Successful only when the sharing of cybersecurity-related information is protected by non-disclosure agreements that remain intact from freedom of information requests filed to force public disclosure,
- Accomplished only when all parties are protected from liability, including antitrust and litigation concerns.

Cybersecurity information sharing *is not:*

- Surveillance or exchange of data among private-sector networks, carriers and/or other industry players and government entities,
- Discussion or collaboration on pricing, markets or any other matter that is viewed as competitive under antitrust law,
- Cooperation for any purpose other than cybersecurity purposes.

The sharing of information may occur among private entities, or it may occur between private and government entities. Different kinds of information sharing may have different implications, and it is important to recognize the distinction when considering the importance of information sharing, the limitations and the remedies.

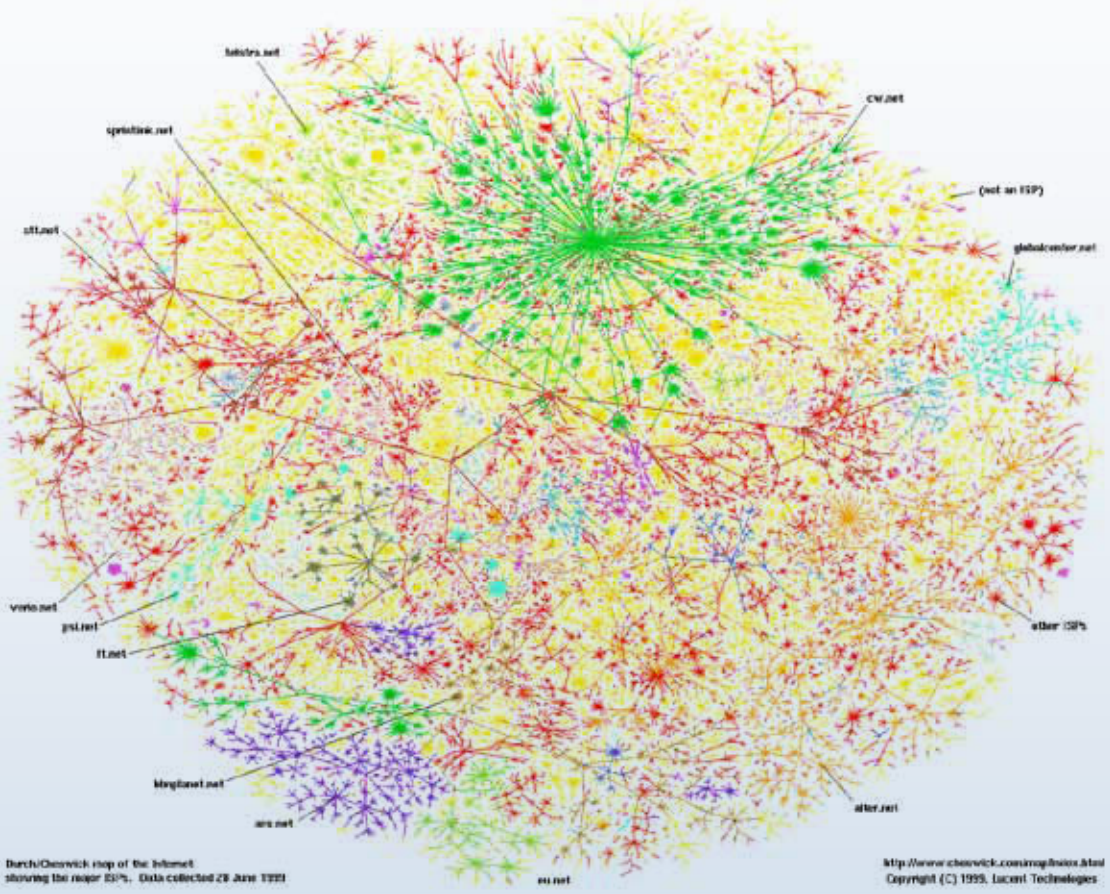
1. Importance of Cybersecurity Information Sharing

Our cybersecurity in large part depends on the strength of the weakest part of a network. We know sharing threat information is critical to effective cybersecurity.

– White House Cybersecurity Coordinator

All security faces the problem of the weakest link. In the cybersecurity realm, this problem is magnified exponentially by the interconnected nature of critical information and communication systems. Today, the communications infrastructure of the United States is connected, thanks to the Internet, to systems all over the world.

Imagine how much more complex the links in the Internet of 2014 are compared with this well-known depiction of the Internet based on a data mapping exercise from 1999. The challenge of maintaining secure networks for the safe exchange of data is vastly more difficult today and, one can assume, will be even greater in future years as the connections continue to expand and technology provides us with even more ways to connect and communicate.



Every company involved in the wireless broadband industry must have access to the latest intelligence gathered by U.S. cybersecurity experts on emerging threats, and the latest innovations in responses and protections if the nation's highly interconnected digital ecosystem is to stay sufficiently secured to maintain the trust of end users and consumers.

The importance of cybersecurity information sharing, as defined here, cannot be overstated. Even though it takes place below the surface of what we typically understand as cybersecurity communications, it serves as the essential, hidden shield in the ongoing struggle to protect our mobile devices, laptops and wireless Internet-based services against cyberthreats.

As three cybersecurity experts in the U.S. military recently wrote on the need for improvements in public-private cybersecurity information sharing —

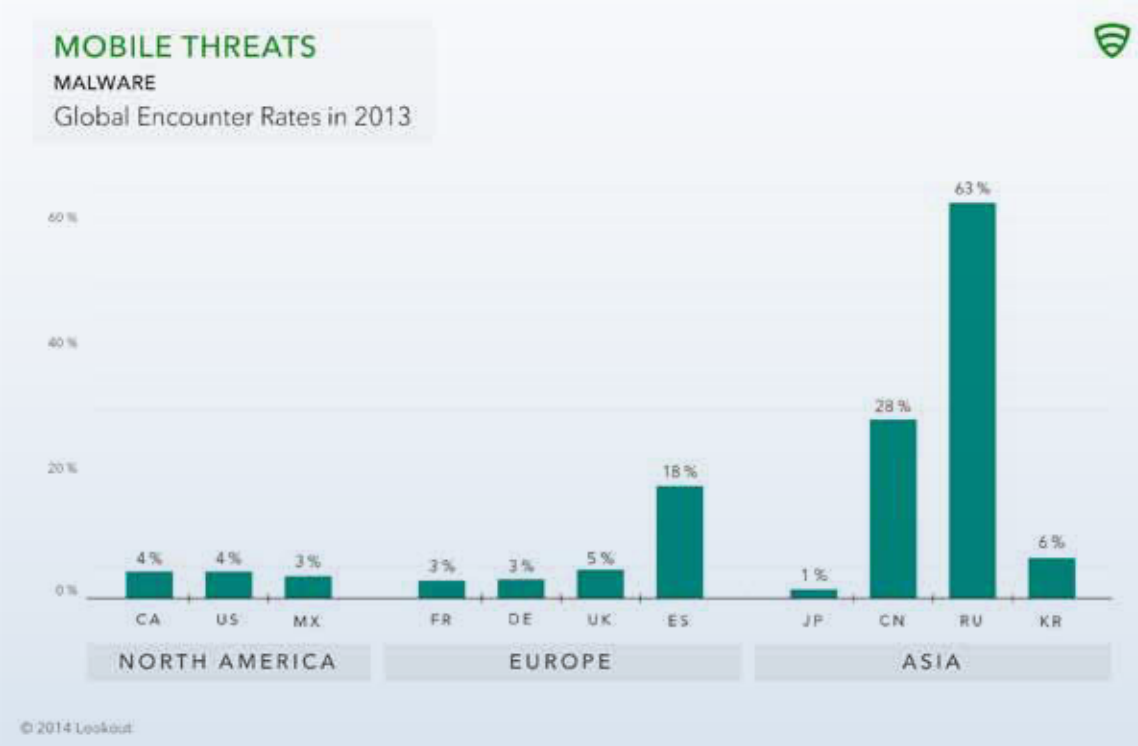
Since nongovernmental entities own and operate a large majority of cyberspace and critical infrastructure, the United States needs not only a whole-of-government approach to cybersecurity, but also a whole-of-nation approach.[3]

2. Contributions of Information Sharing to Mobile Cybersecurity

In the United States, advances in structured cybersecurity information sharing over the past decade, beginning after the terrorist attacks of September 11, 2001, are evident in the relatively low rates of malware encounters in this country as compared with much of the rest of the world.

In general, the mobile malware encounter rate in the U.S. averages four percent, while in Russia and China it is 63 percent and 28 percent, respectively.[4] This continued low encounter rate is an important gauge of the success of the wireless communications industry's track record on cybersecurity and the strength of the industry's participation in cybersecurity information sharing. This chart illustrates the encounter rates of mobile cyberthreats in 2013 for North America, Europe and Asia.

Source: Lookout, Mobile Threats, Made to Measure (2014)



Evolution of Information Sharing

Efforts to improve information sharing—in many instances basic communication—among military and civilian government organizations have been accelerated as security crises and major disasters occurred, whether natural or man-caused. For example, the National Communications System (NCS) was created within the Department of Defense (DoD) following the Cuban missile crisis in 1962, after communications problems arose among the United States and its allies and the Soviet government, which threatened to worsen the situation.

Now in the age of the Internet, the National Coordinating Center (NCC), originally part of NCS and governed now by the Department of Homeland Security (DHS), is one of the primary forums for industry and government to share information on cyberthreats and attacks. It is among the major changes made to improve government-industry security information sharing since the September 11, 2001 terrorist attacks.

Following 9/11, a renewed push for improved information sharing began, with mandates for government agencies to create a methodology for regularly sharing relevant information within government, and to establish formal ties with industry sectors that control critical infrastructure that might be threatened by terrorists. Americans and their leaders learned that when information is hoarded, those needing it may not be able to respond in a timely fashion.

Much has changed since the Cold War era. Eighty percent of modern U.S. critical infrastructure, including that which supports U.S. wireless broadband communications, is in private sector hands, and the 20 percent under government control cannot be managed effectively separate, as these public and private networks and systems are deeply interconnected within the Internet.

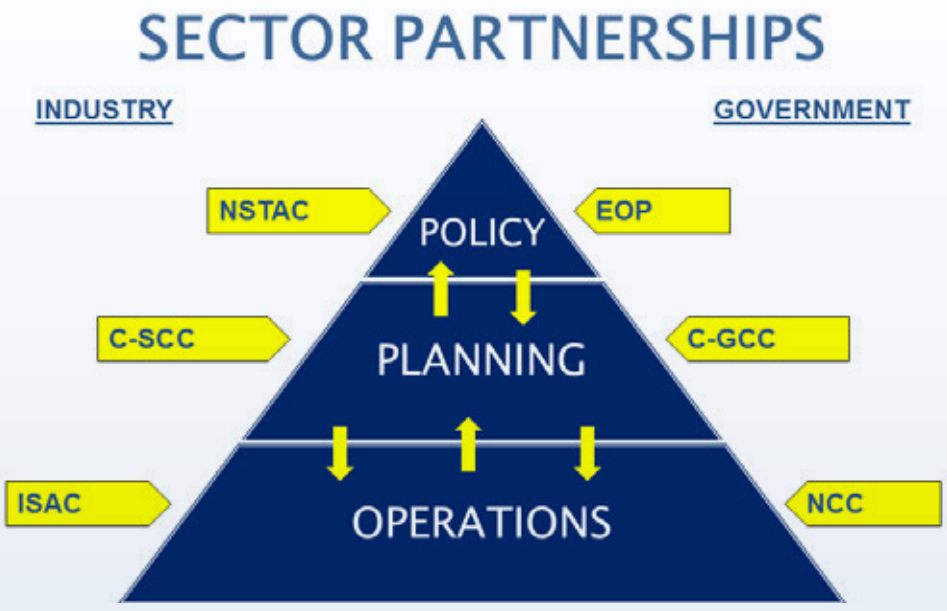
The 9/11 attacks, followed by natural disasters such as Hurricane Katrina, spurred more extensive government efforts to build information-sharing processes with every industry segment controlling critical infrastructure, including the nation's wireless broadband industry as part of the communications industry sector.

So far, however, the emphasis has been on creating administrative structures and adding more regulations rather than developing the legislative reforms needed to support a modern cybersecurity platform for information sharing.

Public-Private Partnerships

Central to the new cybersecurity information sharing landscape between government and industry are a number of interconnected institutions. The paths along which communications industry sector players can share information among themselves, and with government agencies and organizations, is complex and subject to rigorous controls and limitations.

As part of the industry's ongoing commitment to cybersecurity, CTIA and its members are actively engaged in a number of partnerships both within the industry and with government entities, all with the aim of advancing the security of wireless broadband networks and systems nationwide.



Major groups in the information-sharing landscape for the wireless communications industry include:

NCCIC | National Cybersecurity and Communications Integration Center.

Formed by DHS as it consolidated many watch desks across the agency, the NCCIC was made a component of this major Center, along with the U.S. Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Together, these groups monitor, track, mitigate and address communications vulnerabilities, intrusions, exploits and incidents across all federal agencies and the private sector. A total of 24 federal agencies and over 50 private sector communications and information technology companies routinely share critical communications information and advice in a trusted environment to support this combined national security/emergency preparedness communications mission.

Comm-ISAC | Communications Information Sharing and Analysis Center

Created by a presidential decision directive as the Telecom Information Sharing and Analysis Center (Telecom ISAC) under DHS, its counterpart at the government level is the NCC. Its mission is to enable voluntary collaboration and information sharing on vulnerabilities, threats, intrusions and anomalies from multiple sources, and to perform analysis with the goal of averting or mitigating impact upon the telecommunications infrastructure, including the nation's wireless broadband networks.

CSCC | Communications Sector Coordination Council

Created by DHS, the CSCC is one of 16 industry sector coordination councils established under the Critical Infrastructure Partnership Advisory Council (CIPAC) to ensure communications networks and systems are secure, resilient and rapidly restored after a natural or man-caused disaster.

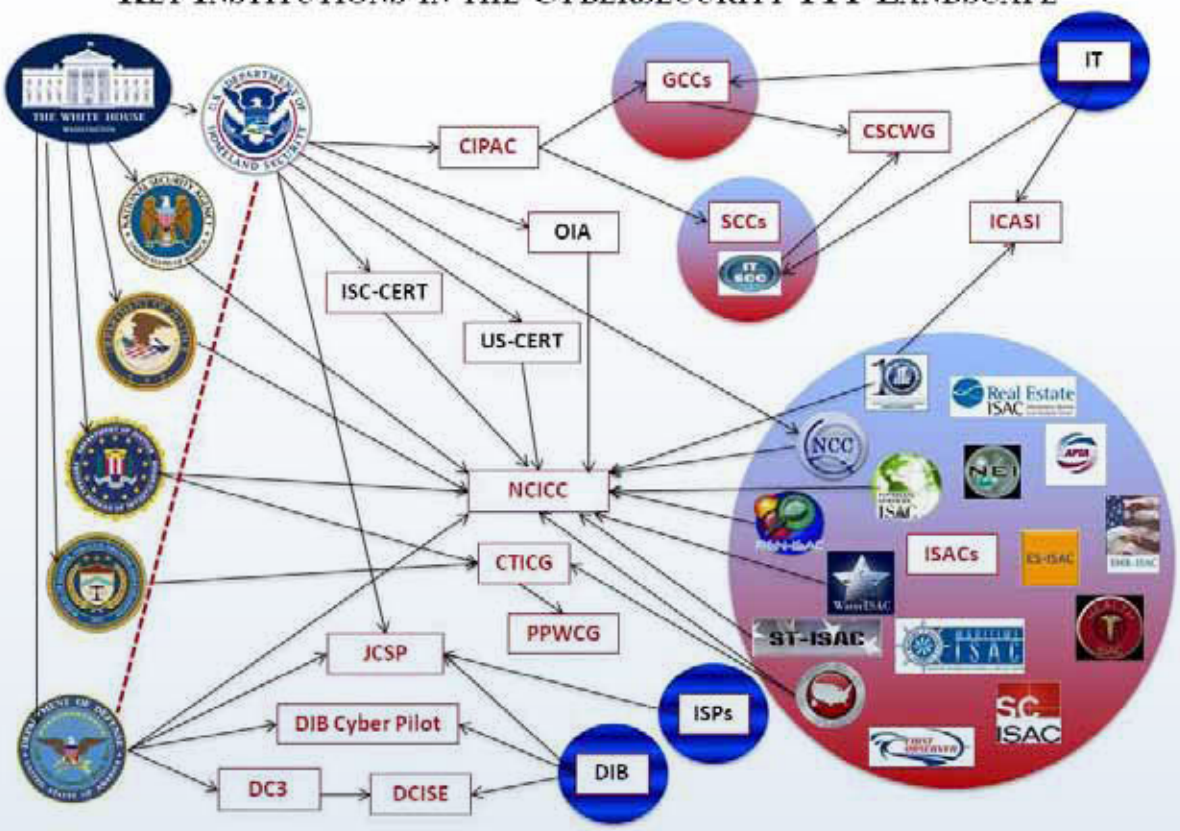
NSTAC | National Security Telecommunications Advisory Committee

Created by Executive Order, its 30+ members are appointed by the president from leading communications, network service and IT companies to make recommendations on industry-government

cooperation needed to respond to cyberattacks of national significance. CTIA's recommendations are provided through its member company participants, as associations are no longer named members.

These public-private partnerships make possible certain exchanges of information related to cybersecurity threats that can impact mobile communications, but face limits, or barriers, based on the current legislative foundation, which was laid down long before data began traveling around the world at hyperspeed.

KEY INSTITUTIONS IN THE CYBERSECURITY PPP LANDSCAPE



Examples of some of the impediments to information sharing:

1. Risk of Public Disclosure (e.g., FOIA);
2. Non-Actionable Threat Information;
3. Timeliness of actionable information because of very demanding regulatory requirements that companies remove various kinds of information before sharing, with the consequence of severe liability for failing to do so, even when the party acts in good faith;
4. Comm-ISAC limitations on private-to-private collaboration about cyberthreats (e.g., DDoS attacks on enterprise customers); and
5. Information classifications (e.g., government classified information).

NIST Cybersecurity Framework

An important new set of principles to guide the future of cybersecurity information sharing came in February 2014, when the National Institute of Standards and Technology (NIST) published the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. It supports information sharing in several important ways by providing a voluntary Framework based on well-established risk management principles.

> *A central component of these risk principles is the appropriate sharing of information both within organizations and among industry segments and government partners.*

The Framework provides business drivers to help guide voluntary cybersecurity activities based on the organization's risk management processes. It uses current industry standards and best practices to lay out a three-part approach:

- **FRAMEWORK CORE —** A set of defined cybersecurity functions: Identify, Protect, Detect, Respond, Recover. Together, these core activities form the strategies for an organization's management of cybersecurity risks. Under each are key categories and subcategories of actions for each function, matched with informative references which include cybersecurity standards. Communications are essential components within the Respond and Recover core functions.
- **FRAMEWORK PROFILE —** A guide for organizations to develop their current cybersecurity profiles, so that opportunities for improvement can be easily identified and prioritized.
- **FRAMEWORK IMPLEMENTATION TIERS —** A scale to provide context to organizations on how they view cybersecurity risks, and the processes they have in place to manage that risk, using a structure of tiers reflecting a progression from informal and reactive, to repeatable and adaptive.

The Framework complements and builds upon existing practices. It will contribute significantly to future voluntary efforts to strengthen cybersecurity information sharing by providing the common language for industry groups, companies and government agencies to use in defining how information sharing can work to advance cybersecurity and protect privacy in a growing threat environment.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The Framework... will contribute significantly to future voluntary efforts to strengthen cybersecurity information sharing...

Heartbleed Bug: *A Case Study*

On April 7, 2014, the same day that a patch was released, the media was informed that researchers identified a serious vulnerability in a widely used OpenSSL cryptographic software library that allowed attackers to access data protected by the Transport Layer Security (TLS) protocol used to secure the Internet. SSL/TLS provides security for applications like email, Web, instant messaging (IM) and some types of virtual private networks (VPNs).

At that time, some 17 percent (around half a million) of the Internet's secure Web servers were believed to be vulnerable to attack by exploiting this weakness, allowing theft of the servers' private keys and users' cookies and passwords.[5]

A Finnish security company quickly gave the weakness a name, Heartbleed, a website and a logo, increasing the public's (and hackers') awareness of this widespread vulnerability.[6]

The result was that companies and governments had to scramble to deploy the patches, change passwords and generally adapt their networks to prevent cyberattackers from exploiting this now widely publicized vulnerability.

3. Limitations and Remedies for Cybersecurity Information Sharing

We need to provide American companies the information they need to better protect their networks from these dangerous cyberthreats.

– Chairman of the House Permanent Select Committee on Intelligence

The foundation of effective cybersecurity information sharing is protections that facilitate the ready and rapid exchange of cybersecurity-related threats, countermeasures and recovery mechanisms in the collective context of the private sector, and rests on three principles:

- Liability protection (with respect to private-to-private and private-to-government sharing);
- Antitrust exemption (with respect to private-to-private sharing); and
- Protection against public disclosure (with respect to private-to-government sharing).

These principles cannot be accomplished by supportive public statements from policymakers or administrative guidance or federal regulations alone. *Legislation* is needed to provide legal certainty, and thereby enable a more real-time, active cybersecurity threat response capability.

Limitations

Carrier companies that are "resident members" with access to reports and controlled documents at NCCIC's Sensitive Compartmented Information Facility (SCIF) cannot share any information that their representatives are given in briefings—even within their own companies, much less with others in the communications industry.

In April 2014, the Department of Justice (DOJ) and the Federal Trade Commission (FTC) announced that "properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns" in an effort to assure private-sector competitors, including the wireless communications industry, of the administration's support for this essential component in the nation's cybersecurity defenses.[7]

However, the DOJ's narrowly defined statement on information sharing in the cyberthreat context does not provide the necessary and comprehensive legal protections required to engage in the serious and ongoing business of cybersecurity information sharing. Only a statutory remedy will close this gap.

Currently, private sector companies cannot share information with a government agency or organization without a) researching to ensure that whatever data is being shared is not protected, sensitive or classified; and b) assuming the risk of the information being made publicly available as a result of a FOIA request.

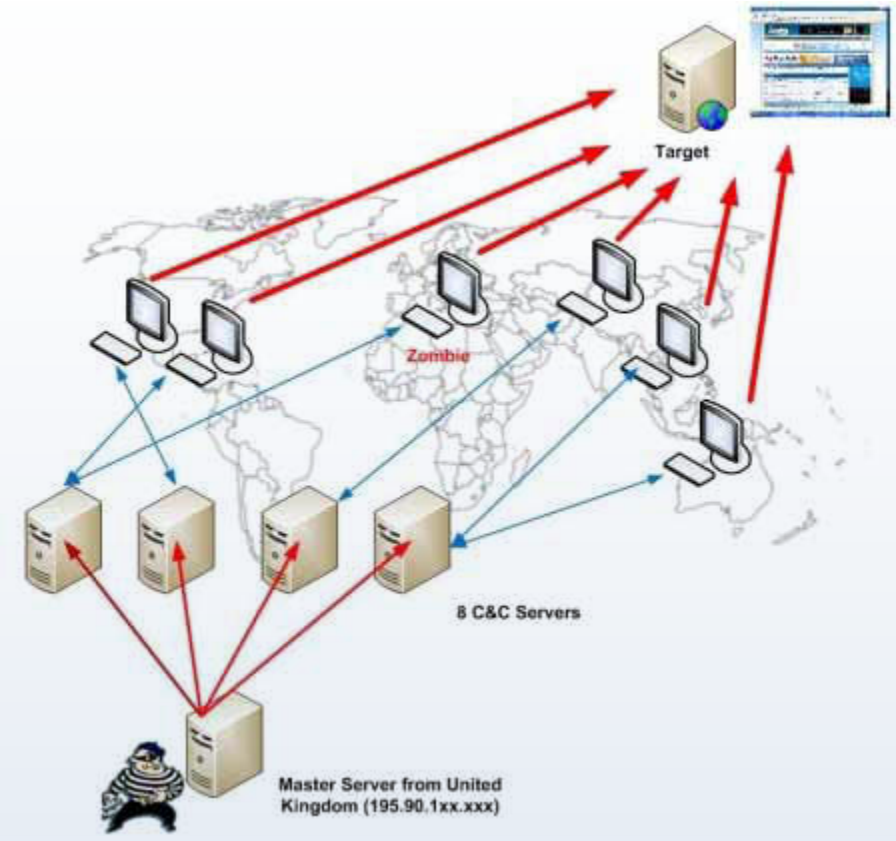
A trio of military cybersecurity experts recently called upon Congress to provide the confidence-building legislative platform needed to encourage industry cybersecurity information sharing:

> *The Obama administration's Executive Order 13636 and Presidential Policy Directive 21 made positive steps toward rectifying many shortcomings. However, these actions represent only a part of the solution. Congress must now act to provide complementary cybersecurity legislation to fill gaps in the public-private information-sharing construct prescribed in the 2003 strategy. Only then will the United States be fully on the path to a whole-of-nation approach to meet the full scope of cyberthreats.*[8]

"properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns"

Four Scenarios Illustrate Current Limitations

There are many circumstances in which information can and should be shared between private parties and with the government. But doing so may expose companies to liability or public disclosure, which chills their ability to collaborate. A few scenarios may help demonstrate some of the current limitations related to sharing information between private sector entities, and also between the private sector and government entities.



The diagram above illustrates a botnet attack against a customer (the target) via a broadband communications carrier, and the following scenarios address aspects of the response and information-sharing that could relate to the attack.

SCENARIO ONE: If the customer requests the carrier to investigate the botnet attack, the carrier can intercede and perform the necessary deep-packet inspection to identify the botnet and mitigate the attack. However, under the current environment, it is unclear if the carrier can share real-time information about the botnet attack with other carriers, and to what extent the information may be shared with similarly affected customers.

SCENARIO TWO: If a government agency requests the carrier to help investigate and share information about the suspicious activity, such as in the case of the Silk Road website take-down by the FBI[9] the carrier may have to decline unless and/or until the government agency supplies a court order or subpoena to share information that may be relevant to the suspected activity.

SCENARIO THREE: Assuming that some information can be shared between private entities and/or with the government, some policymakers would require companies to assure that there is little or no disclosure of Personally Identifiable Information (PII). But cyberthreat information can lose value if its sharing is delayed due to stringent requirements to ensure the removal of PII, with no exception made for good faith efforts to do so. Such a requirement may mean that private entities have to engage in a non-automated, detailed legal review of any data before it is shared. Such a review could take weeks or longer, depending on the quantity of data that is shared.

SCENARIO FOUR: Following up on the attack, a government agency may seek information from the customer and carrier about their experience, their general policies, capabilities and technologies, or best practices. Such information, if provided to the government, can be subject to public disclosure under the FOIA, which provides any person a right, enforceable in court, to obtain access to federal agency records. A FOIA request can be made for any agency record, even those that contain information obtained from the private sector about their views, activities and businesses. Several exceptions may apply to protect certain private information in the government's possession, but those exceptions can be narrow, and their applicability is far from assured.

Disputes often require private entities to intervene in court to protect information from disclosure. The risk of public disclosure under FOIA and the threat of having to litigate to protect information require companies to conduct risk-benefit analyses, and ultimately, they may decide to not share information with the government.

These simplified examples are just some of the many ways that legal and regulatory obligations can hamper vital information-sharing.

Remedies

Communications industry groups, including CTIA, National Cable & Telecommunications Association (NCTA), and U.S. Telecom Association (USTA), are recommending that cybersecurity legislation affirmatively address the three principles of protection described here, and establish the foundation on which productive information sharing can take place.

This includes addressing concerns about potentially providing open-ended authorizations for sharing and collaboration between government and industry, by incorporating legislative language that does the following:

1. Permits and protects information sharing for defined "cybersecurity purposes;"
2. Makes clear that authorized cybersecurity countermeasures can only be employed on a private entity's network or customer network with written customer authorization;
3. Provides protection for companies taking reasonable steps to prevent disclosing to the US government information that is not necessary to respond to a cyberthreat.

These legislative remedies dovetail with the industry's long-advocated recommendation that the federal government maintain regulatory flexibility and refrain from requiring specific technology solutions or prioritizing different privacy or security rules based on the technology used. Such approaches would defeat the very goal we all seek—advancing security and privacy protections against increasingly adaptive threats and converging technologies.

Why is this so important? It's because of the speed with which cyberthreats adapt and advance. In less than a year, cross-platform threats have begun to appear that can target devices that use different hardware platforms, different operating systems and attack across wireline or wireless systems.

As one security expert said recently: "Writing attacks that target more platforms is smart business for criminals—they might as well hit as many users as possible. Why stop with just Windows when you can hit Mac, Linux and mobile too?"[10]

...attacks that target more platforms is smart business for criminals...

The constantly changing nature of cyberthreats demands regulatory flexibility because it supports the adaptability that the wireless industry needs to continue to create innovative cybersecurity and privacy solutions. Only a legislative remedy can create the protections and confidence the private sector needs to engage fully in cybersecurity information sharing in today's mobile environment.

Endnotes

1. *National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014, available at* **http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf**

2. *Sharing Threat Intelligence to Mitigate Cyber Attacks, TM Forum, October 2013*

3. *Veronica A. Chinn, Lee T. Furches, and Barian A. Woodward, Information-Sharing with the Private Sector,, Joint Force Quarterly, 2d Quarter 2014, available at* **http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_32-38_Chinn-Furches-Woodward.pdf**

4. *Lookout, Mobile Threats, Made to Measure, Feb. 2014, available at* **https://www.lookout.com/resources/reports/mobile-threat-report**

5. *Paul Mutton, Half a million widely trusted websites vulnerable to Heartbleed bug, Netcraft Ltd., April 8, 2014, available at* **http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html**

6. *John Biggs, Heartbleed, The First Security Bug With A Cool Logo, TechCrunch, April 9, 2014, available at* **http://techcrunch.com/2014/04/09/heartbleed-the-first-consumer-grade-exploit/**

7. *U.S. Justice Department media release, Federal Trade Commission Issue Antitrust Policy Statement on Sharing Cybersecurity Information, April 10, 2014, available at* **http://www.justice.gov/opa/pr/2014/April/14-at-365.html**. *See also Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information (April 10, 2014), available at* **http://www.justice.gov/atr/public/guidelines/305027.pdf**

8. *Chinn, Furches, and Woodward, Information-Sharing with the Private Sector, op cit.*

9. *Jose Pagliery, FBI shuts down online drug market Silk Road, CNN Money, October 2, 2013, available at* **http://money.cnn.com/2013/10/02/technology/silk-road-shut-down/index.html**

10. *Mikko Hypponen, Chief Research Officer at F-Secure Labs, The Threats are Cross-Platform – And So Is Our Technology, F-Secure Labs, available at* **http://www.f-secure.com/en/web/corporation_global/news-info/product-news-offers/view/story/886491/The%20Threats%20are%20Cross-Platform%20%E2%80%93%20And%20So%20Is%20Our%20Technology**

WWW.CTIA.ORG