Cybersecurity Risk Management Best Practices (WG 4)

Cybersecurity Framework for the Communications Sector

Presentation to Information Security and Privacy Advisory Board (ISPAB)

October 23, 2014

Co-Chairs:
Robert Mayer, USTelecom
Brian Allen, Time Warner Cable

Content

- Project Origins/Synchronicity
- Project Description
- Working Group Composition
- Project Work Streams/Timeline
- Analytical Illustrations (Draft Works-In-Progress)
- Next Steps

Synchronicity

Executive Order 13636 – February 2013

CSRIC IV Chartered - March 2013

NIST Cybersecurity Framework 1.0 – February 2014

WG 4 Cybersecurity Best Practices – Begins March 2014

Project Description*

In order to provide for confidence in the resilience and reliability of the **core public communications functions** in the face of cyber threats. Working Group 4 will develop **voluntary mechanisms** to provide macro-level assurance to the FCC and the public that communications providers are taking the necessary **corporate and operational measures to manage cybersecurity risks** across the enterprise. The macro-level assurance will demonstrate how communications providers are reducing cybersecurity risks **through the application of the NIST Cybersecurity Framework, or an equivalent construct.**

These assurances:

(1) can be tailored by individual companies to suit their unique needs, characteristics, and risks (i.e., **not one-size-fits-all),**
(2) are based on meaningful indicators of successful (and unsuccessful) cyber risk management (i.e., outcome-based indicators as opposed to process metrics), and
(3) allow for **meaningful assessments both internally (e.g., CSO and senior corporate management) and externally** (e.g., business partners).

* (**Emphasis added)**

WG 4 Leadership Team

WG4 Leadership Team

- Co-Chairs: Robert Mayer, USTelecom and Brian Allen, Time Warner Cable
  - Segment Leads
    - Broadcast, Kelly Williams, NAB
    - Cable, Matt Tooley, NCTA
    - Wireless, John Marinho, CTIA
    - Wireline, Chris Boyer, AT&T
    - Satellite, Donna Bethea Murphy, Iridium
  - Feeder Group Initiatives
    - Barriers to Implementation, Co-Leads, Harold Salters T-Mobile, Larry Clinton, Internet Security Alliance
    - Mids/Smalls – Co-Leads, Susan Joseph, Cable Labs, Jesse Ward, NTCA
    - Top Cyber Threats and Vectors - Russell Eubanks, Cox, Joe Viens, TWCable
    - Ecosystem – Shared Responsibilities, Co-Leads, Tom Soroka, USTelecom, Brian Scarpelli, TIA
    - Measurement, Co-Leads, Chris Boyer, AT&T, Chris Rosenraad, TimeWarnerCable

Advisors

- Donna Dodson, WG4 Senior Technical Advisor, NIST, Deputy Chief Cybersecurity Advisor & Division Chief for Computer Security Division
- Lisa Carnahan, NIST, Computer Scientist
- Emily Talaga, WG4 Senior Economic Advisor, FCC
- Tony Sager, Council on Cybersecurity

Engineering and Operational Review

- Lead - Tom Soroka, USTelecom
- Segment Leads Support

Drafting Team

- Co-Leads – Stacy Hartman, CenturyLink, Robert Thornberry, Alcatel/Lucent, Paul Diamond, CenturyLink

WG4 Membership Team

106 members representing the communications sector, and representatives from the energy, financial and IT sectors, standards bodies, vendors, as well as federal and state departments and agencies.

Robert Mayer (Co-Chair)
Brian Allen (Co-Chair)
Samara Moore (Sr Policy Advisor)
Donna Dodson (Sr Tech Advisor)
Emily Talaga (Sr Economic Advisor)
Vern Mosley (FCC Liaison)
Adrienne Abbott
Anthony Acosta
Michael Alagna
Carl Anderson
Sohail Anwar
Nadya Bartol
James Bean
Chris Boyer
Chuck Brownawell
Lois Burns
Ingrid Caples
Joel Capps
Lisa Carnahan
Dan Cashman
William Check
Nneka Chiazor
Andre Christian
Larry Clinton
Edward Czarnecki
Andrew D'Uva
Shelton Darensburg
Kate Dean
Daniel Devasirvatham
Paul Diamond
Martin Dolly
Tanner Doucet
Seton Droppers
Vinit Duggal
Victor Einfeldt
Russell Eubanks
Paul Ferguson
Rick Foster
Craig Froelich
Inette Furey
Chris Garner
Michael Geller
Jessica Gulick
Stacy Hartman
Mary Haynes
Alex Hoehn-Saric
Chris Homer
Charles Hudson, Jr
Wink Infinger
Chris Jeppson
Susan Joseph
Franck Journoud
Merike Kaeo
Aniruddha R. Karmarkar
Kevin Kastor
John Kelly
Scot Kight
Danielle Kriz
Rick Krock
Greg Kulon
Jeremy Larson
Adam Levy
Greg Lucak
Ethan Lucarelli
John Madden
Daniel Madsen
Jennifer Manner
John Marinho
Beau Monday
Donna Bethea Murphy
Paul Nguyen
Jorge Nieves
Mike O'Hare
Michael O'Reirdan
Glen Pirrotta
Martin Pitson
Joel Rademacher
J. Bradford Ramsay
Alan Rinker
Chris Roosenraad
Robert Ross
Tony Sager
Harold Salters
Brian Scarpelli
Karl Schimmeck
J. J. Shaw
Ray Singh
Tom Soroka
Craig Spiezle
Bill Taub
Robert Thornberry
Matt Tooley
Fred Travis
Bill Trelease
Colin Troha
Danna Valsecchi
S. Rao Vasireddy
Phil Venables
Joe Viens
Christian Vogler
Jesse Ward
Errol Weiss
Kathy Whitbeck
Kelly Williams
Shawn Wilson
Pamela A. Witmer

WG4 Structure

Each industry segment analyzes cyber risk management practices -- and informed by the feeder groups -- adapts the NIST Cybersecurity Framework (CSF) for voluntary use for their segment

- Barriers & Other Considerations
- Small and Medium Business
- Top Cyber Threats And Vectors
- Ecosystem & Shared Responsibility
- CSF Success Indicators (Measurement)

Phase 1: Segment and Feeder Development

Phase 2: Integration & Analysis

Phase 3: Drafting/NIST Feedback

November Initial Draft

Interim Report Jan. 2015

Entering Full Integration Phase

BROADCASTING

There are more than 14,000 radio and 1,700 television broadcasting facilities in the United States, sending broadcasts through the air to a frequency network of transmitters.

CABLE

The cable industry is composed of approximately 7,791 cable systems that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service.

WIRELESS

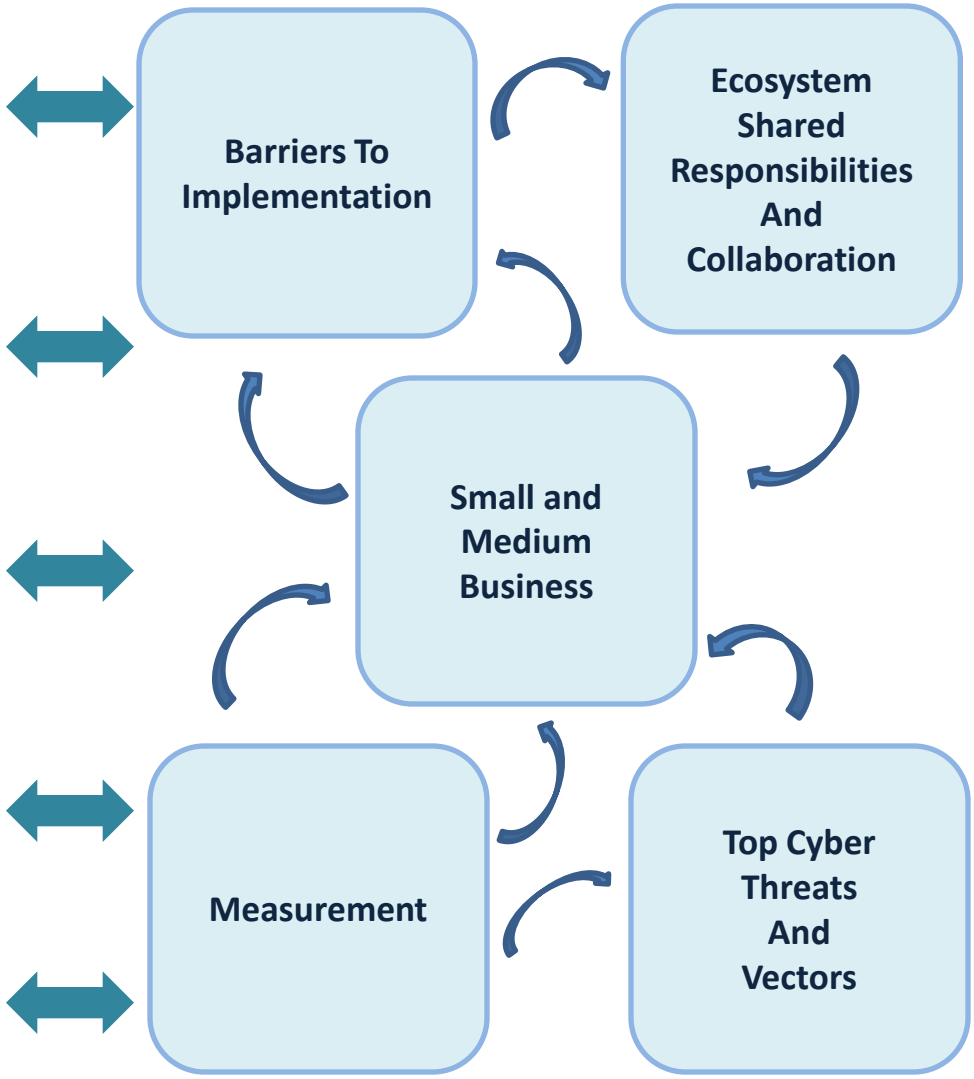
Wireless technology consists of cellular phone, paging, personal communications services, high-frequency radio, unlicensed wireless and other commercial and private radio services.

WIRELINE

Over 1,000 companies offer wireline, facilities-based communications services in the United States. Wireline companies serve as the backbone of the Internet.

SATELLITE

Satellite communications systems deliver advanced data, voice, and video communications, transmitting data from one point on the Earth to another.

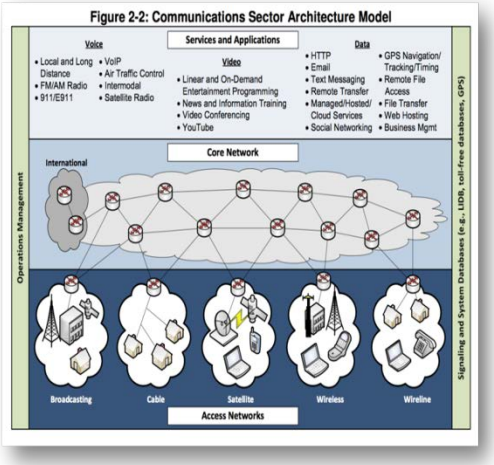


Sample Draft Analytical Illustrations

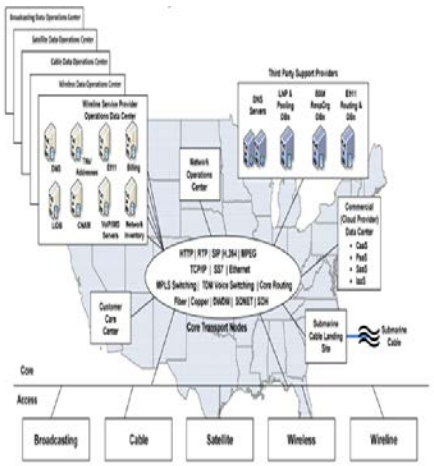
- Scoping Exercise
- Prioritization Methodology
- Ecosystem Considerations/Shared Responsibilities/Dependencies
- Barriers to Implementation
- Small Medium Business
- Threats
- Measurement

2012 NSRA Leveraged for Scoping Purposes

2012 National Sector Risk Assessment for Communications



The wireline segment is focusing their primary efforts on ensuring the reliability and integrity of wireline core infrastructure that supports a wide variety of communications services including voice (both TDM voice and VoIP) and data services.



In addition the wireline segment reviewed the framework in relation of how practices could also be applied to ensure mission critical emergency communications services such as 911 or E911.

Prioritization Methodology

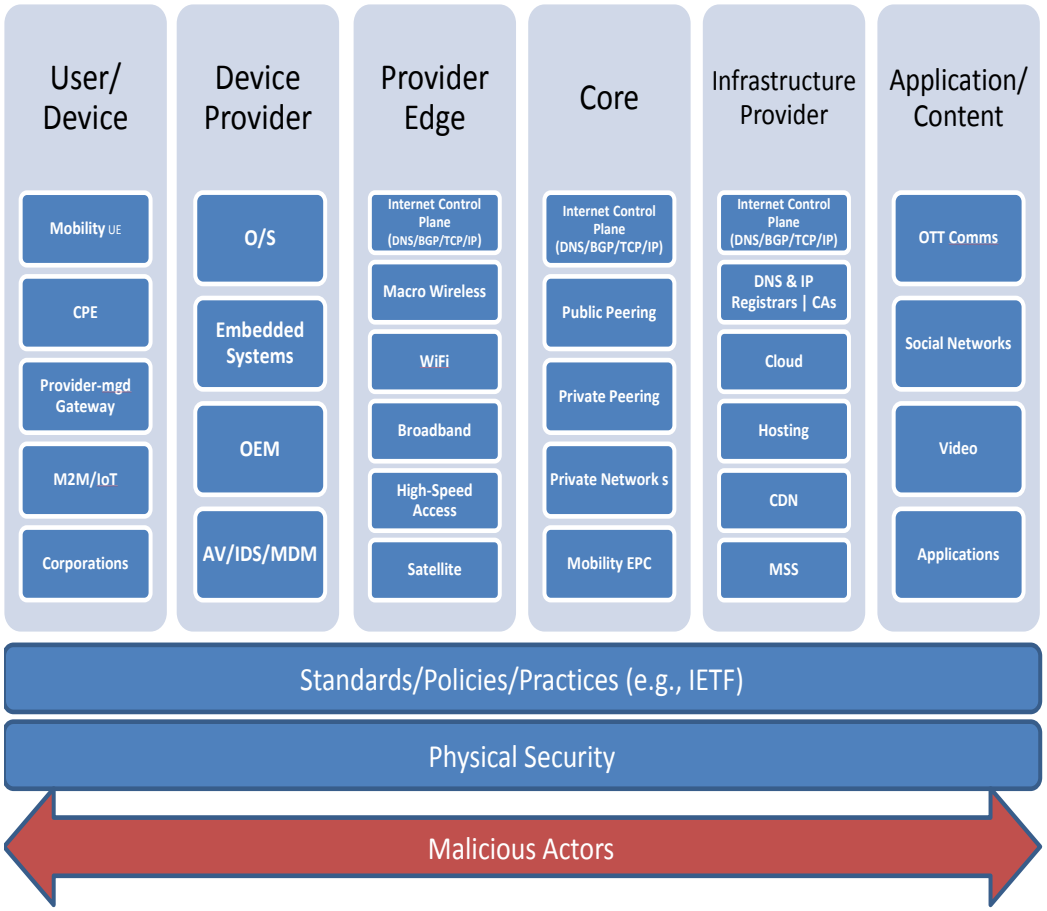
The Wireline Segment group analyzed each of the NIST framework's functional areas, categories and subcategories and assessed them on a variety of factors including whether each functional area, category and sub-category is in or out of scope; how they may be applied; their criticality to protecting against cyber threats (considering input from the threats feeder group); and difficulty to implement (considering input from the barriers feeder group including technological barriers, scale barriers, consumer/market barriers, operational barriers, and legal/policy barriers).

	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
Sub-Category (only as needed)	Is the function, category, sub-category in scope as a best practice for the critical infrastructure "systems and assets" determined by the sub-group (wireline, wireless, satellite, broadcast or cable)? (In-scope or Out-of-Scope).	Explanation of how the function, category, subcategory applies to the critical infrastructure as defined by the sub-group (wireline, wireless, satellite, broadcast or cable).	Criticality of the given function, category and subcategory on scale of 1 to 5 by segment. (Scale: 5= Extremely Critical, 4 = Very Critical, 3= Somewhat Critical, 2 = Slightly Critical, 1 = Not at all Critical).	Difficulty for the implementation of the function, (Includes factors such as costs and barriers to implementation). (Scale: 5= Not at all Difficult, 4 = Slightly Difficult, 3= Somewhat Difficult, 2 = Very Difficult, 1 = Extremely Difficult).
ID.AM-1: Physical devices and systems within the organization are inventoried	In Scope	Sub-category should be applied to critical infrastructure assets or more broadly as part of cyber risk management at the firms discretion.	5	2

Ecosystem Considerations

U.S. Communications Sector Coordinating Council

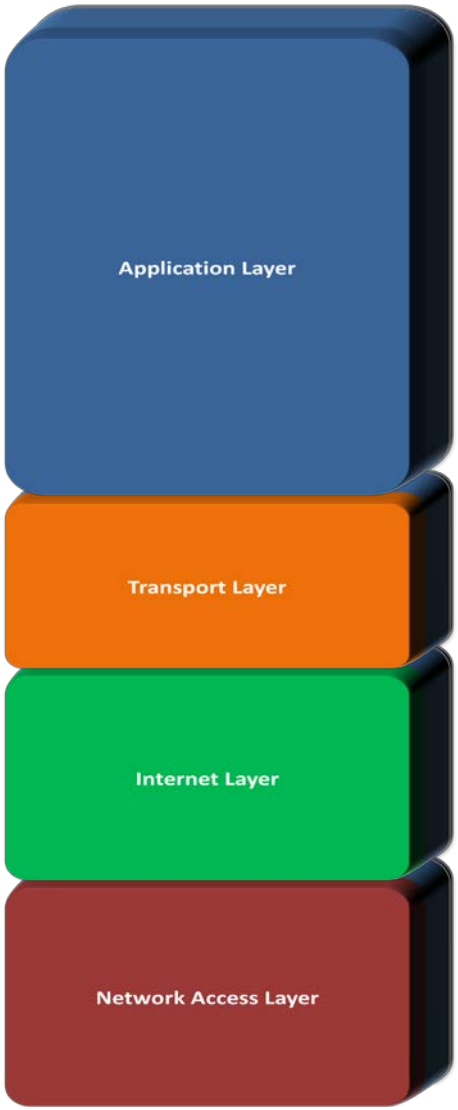
Cyber Ecosystem Players



One of the more comprehensive 'Ecosystem' diagrams, comes from a joint industry/government partnership called the U.S. Communications Sector Coordinating Council (CSCC). The Ecosystem Feeder group determined that this diagram captured a large number of the categories of the Ecosystem that were previously identified and it was an excellent depiction of the various 'Cyber' Ecosystem relationships within the Communications Sector.

CSRIC Communications Security, Reliability and Interoperability Council

Ecosystem Considerations (Continued)



Identified the major network and computing protocols that resided in each of the TCP/IP model layers.

Mapped known cyber attacks, threats and breaches to specific layers of the TCP/IP model, based on what protocols or layers were attacked and exploited.

Barriers to Implementation

Barriers to Implementation and Other Considerations				
Technological Barriers	Scale Barriers	Consumer/Market Barriers	Operational Barriers	Legal/Policy Barriers
Are there key systems/tools/products (technology) generally available that support this risk management activity?	Does the capability scale with organizational growth and change?	Does this risk management capability conflict with consumer or market needs?	Are there recognized barriers to implementing this risk management activity?	Are there any legal, regulatory or policy impediments (e.g., privacy, anti-trust, and tort liabilities) to implementing this recommendation? Will this process benefit from incoming /outgoing information sharing?

Relevant Categories	Barriers Discovered/Mitigation Opportunities
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**Operational:** **Operational:** **Technology:** **Consumer/Market:** **Legal/Policy:** **Financial:** Barriers are dependent on the size of an organization, and costs are not linear. Marginal cost for improving Tier position is often exponential. Nonetheless, enterprises should use the NIST framework's Tier definitions to determine their current posture, and where they want to be.

This analysis is the basis for individual enterprises to assess the hurdles they must consider when implementing any of the 98 sub-categories. These hurdles can vary dramatically by company depending on a variety of factors including their ability to recover for investments in security, the current state of their cyber capabilities, and the priority placed on these efforts by top management.

Small Medium Business

The objective here is to provide practical guidance to small and medium size businesses who more often than not lack the skill sets and resources of larger corporate enterprises. It is also important to recognize that, while many small companies may lack scale, they often possess the intellectual capital and vision that places them at the forefront of cybersecurity advances.

Web-based Resources for SMB

DESCRIPTION	SOURCE	TITLE	LINK
This report assists small business management to understand how to provide basic security for their information, systems, and networks.	NIST	Small Business Information Security: The Fundamentals	http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf
Provides tips for creating and maintaining strong passwords.	Microsoft	Tips for creating strong passwords	http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password
Provides instructions, recommendations, and considerations for creating a contingency plan that is used government agencies but can be applied to any company/industry.	NIST	Contingency Planning Guide for Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
A tool for small businesses to create customized cyber security planning guides.	FCC	FCC Cyber Security Planning Guide	http://transition.fcc.gov/cyber/cyberplanner.pdf
This document assists organizations in establishing computer security incident response capabilities and handling incidents.	NIST	Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. This site also provides a link to self-assessment tool.	DHS and US-CERT	Cyber Resilience Review (CRR)	https://www.us-cert.gov/ccubedvp/self-service-crr
An organization within DHS responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.	US-CERT	United States Computer Emergency Readiness Team	https://www.us-cert.gov/
Resources to help businesses align themselves to the five Cybersecurity Framework Function Areas.	DHS Critical Infrastructure Cyber Community (C³)	Getting Started for Business	https://www.us-cert.gov/ccubedvp/getting-started-business

The SMB feeder group will advance awareness and education with regard to the importance of cybersecurity for small and medium-sized organizations and work to ensure that cybersecurity risk management "best practices" are flexible and scalable for companies of all sizes. As such, the SMB feeder group's objectives are as follows:

- Explain, in basic terms, why cybersecurity is important and what SMBs can achieve by using the WG 4 document to improve their cybersecurity risk management practices.
- Provide overall guidance on how SMBs can digest and use the NIST Framework.
- Provide guidance with respect to prioritization of relevant subcategories from an SMB perspective.
- Develop at least one SMB use case.
- Identify barriers, in coordination with the Barriers to Implementation feeder group, that SMBs commonly face and explore ideas for mitigating them.
- Develop an annotated, refined list of resources/references/tools for SMBs.

Next Steps

- Complete and refine the ten segment and feeder group reports by early November 2014.
- Ensure that all feeder groups and segments have the appropriate level of engagement and can benefit from "best-in-class" analysis and drafting.
- The Leadership team and the drafters will ensure consistent quality across the entire effort and that the final report will serve as a significant contribution to advancing the CSF initiative.
- Develop findings and conclusions that produce meaningful recommendations for the FCC, other federal agencies, industry, and other key stakeholders.