The Communications Security Reliability and Interoperability Council (CSRIC) Report on Cybersecurity Framework

Presentation to the
Internet Security and Privacy Advisory Board
June 11, 2015

Robert Mayer
VP Industry and State Affairs, USTelecom
CSRIC V Council Member
CSRIC IV WG 4 Co-Chair
CSCC Cybersecurity Committee Chair

Agenda

- Policy Roadmap
- Project Charge
- Approach and Structure
- Assurances
- Guidance
- Recommendations
- Current Activities

Cybersecurity Policy Roadmap

Enterprise-Level Cybersecurity Risk Management

CSRIC Cybersecurity Best Practices - March 2015

WG 4

Executive Order 13636 February 2013

NIST Cybersecurity Framework 1.0 – February 2014

Critical Infrastructure Cyber Community C³ Voluntary Program

Working Group 4 Charge

Develop voluntary mechanisms which give the FCC and the public assurance that communications providers are taking the necessary steps to manage cybersecurity risks across the enterprise;

Such 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).

Demonstrate how communications providers can reduce cybersecurity risks through the application of the NIST Cybersecurity Framework, or an equivalent construct**.**

Develop implementation guidance to help communications providers use and adapt the Cybersecurity Framework developed last year by the National Institute of Standards and Technology (NIST).

Approach and Structure

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

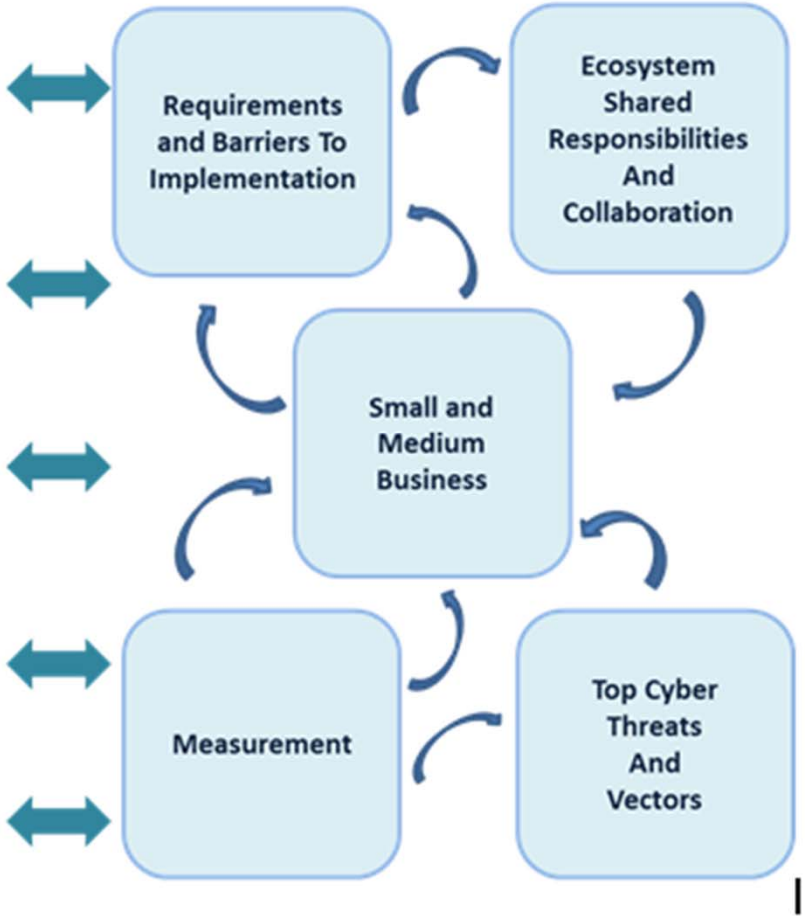
Wireless technology consists of cellular phone, paging, personal communications services, high-frequency radio, unlicensed wireless and other commercial and private radio services.

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.



Approach and Structure

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
    - Requirements and 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, Center for Internet Security

Engineering and Operational Review

- Co-Leads - Tom Soroka, USTelecom and John Marinho, CTIA
- Segment Leads Support

Drafting Team

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

Assurances

Assurances: WG4 was tasked with developing voluntary mechanisms which give the FCC and the public assurance that communications providers are taking the necessary steps to manage cybersecurity risks across the enterprise.

As evidence of the Communication's Sector's commitment to enhance cybersecurity risk management capabilities across the sector and the broader ecosystem, and to promote the use of the NIST CSF, WG4 recommended the following three new voluntary mechanisms to provide the appropriate macro-level assurances.

FCC initiated confidential company-specific meetings, or similar communication formats to convey their risk management practices. The meetings would be covered by protections afforded under the Protected Critical Infrastructure Information (PCII) administered by the Department of Homeland Security (DHS);
A new component of the Communications Sector Annual Report that focuses on segment-specific cybersecurity risk management, highlighting efforts to manage cybersecurity risks to the core critical infrastructure; and
Active and dedicated **participation in DHS' Critical Infrastructure Cyber Community C^3 Voluntary Program,** to help industry increase cybersecurity risk management awareness and use of the Framework.

Guidance

Guidance: Charged with providing implementation guidance to facilitate the use and adaptation of the voluntary NIST Cybersecurity Framework by communications providers, the WG4 members developed and applied a variety of analytical tools and methods that could serve as a primer for companies when reviewing their own risk management processes.

The WG4 Final Report provides significant segment-specific direction based on illustrative examples of how the NIST five functions, 22 categories and 98 sub-categories fall within or outside the scope of applicable critical infrastructure and how processes may be prioritized.

In addition , WG4 concluded that it is essential to incorporate a risk governance process into a cybersecurity program. The key objective is to ensure that an inclusive, independent, and holistic assessment of the current and future enterprise risk posture is routinely undertaken, and to align the enterprise's business mission with sound and effective cybersecurity practices, protocols, and tools.

Recommendations

Recommendations: Consistent with its role as a FACA advisory group. Working Group 4 members made a series of recommendations to the FCC to further the effectiveness of coordination with industry and its government partners. Selected recommendations included:

1. CSRIC recommends that the FCC leverage the resources and capabilities of the three primary communications sector organizations (i.e. NSTAC, CSCC/GCC, Comm-ISAC) to promote voluntary participation in risk management initiatives across all communications segments and providers.

2. CSRIC recommends that the FCC promote the sustained voluntary collaboration and facilitate the sharing of cybersecurity threat information. This can be accomplished by working with the communications sector members and other relevant agents of the U.S. government to identify and mitigate technical, operational, financial, and legal barriers to cyber information sharing.

3. CSRIC recommends that the FCC further explore the considerations and accommodations that are required for SMB's to implement the NIST Cybersecurity Framework and provide macro-level assurances to the FCC and the public.

4. CSRIC recommends that the FCC work to coordinate and rationalize Framework related federal/state government initiatives to ensure efficient use of critical and scarce cybersecurity resources.

Recommendations (Continued)

5. CSRIC recommends that the FCC further incorporate an understanding of the changing threat landscape, sector ecosystem dependencies, and harmonization into previous CSRIC best practices and the NIST CSF.

6. CSRIC recommends that the FCC adopt availability of the critical communications infrastructure as the meaningful indicator of cybersecurity risk management.

7. CSRIC recommends that the FCC continue to collaborate with NIST and DHS in the further development of the NIST CSF and the promotion of programs to increase the voluntary use of the CSF.

8. CSRIC recommends that the FCC partner with other departments and agencies to promote education and awareness of the cybersecurity risks inherent in critical communications infrastructures, and to promote steps that the communications sector can take to give external stakeholders with macro-level assurance that these collective actions are successfully managing cybersecurity risks.

9. CSRIC recommends the FCC promote an industry threat intelligence handling model (referenced in this report), or an equivalent construct by organizations intending to use threat intelligence to maintain cybersecurity, protect critical infrastructure, and protect critical data from rapidly evolving cyber threats.


THANK YOU