Communications sector adopts first-of-its-kind cybersecurity measures

James J. Giszczak | Monday, March 30, 2015

For the first time, the communications industry has critical guidance and recommendations for cybersecurity protection. That's because a multidisciplinary group formed by the Federal Communications Commission (FCC) examined the cybersecuity risks to the communications sector and adopted an extensive 415-page report that contains first-of-its-kind cybersecurity measures for the communications industry to follow. This report – "**Cybersecurity Rick Management and Best Practices Working Group 4: Final Report**" (Report) – was issued on March 18, 2015, by the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC). The Report is expected to be an important tool for other industries looking to implement measures to guard against cybersecurity risks.

Origins of the Report

The origins of the Report date back to 2013 when the FCC created Working Group 4 (WG4) under the CSRIC. That year, President Obama also issued **Executive Order 13636 – Improving Critical Infrastructure Cybersecurity**, which directed the creation of a voluntary public-private partnership with the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. After NIST released NIST CSF Version 1.04 that identified 16 Critical Infrastructure sectors, including the communications sector, WG4 got to work on the Report. Subsequently, in February 2014, NIST released its "**Framework for Improving Critical Infrastructure Cybersecurity**" (Framework).

Focus of the Report

To create the Report, WG4 organized itself into five segment subgroups representing the five key parts of the communications industry:

1. Broadcast
2. Cable
3. Satellite
4. Wireless
5. Wireline

WG4 also established five “feeder” subgroups to engage in a deeper, more focused analysis of subject matter areas that would help the communications sector segments evaluate their cybersecurity risk environment, posture, and tolerance. The following five “feeder” topics were examined to ensure the voluntary mechanisms and sector guidance were grounded in facts, thoughtful judgments, and were practical in their design:

1. Cyber ecosystem and dependencies
2. Top threats and vectors
3. Framework requirements and barriers
4. Small and medium businesses
5. Measurements

WG4’s charge included developing voluntary mechanisms for the communications sector that would provide assurances to the FCC and the public that the communications sector is taking the appropriate steps to address cybersecurity risk. The point is that such “macro-level” assurances would enable organizations in the communications sector to conduct “meaningful” assessments internally as well as with external partners and vendors.

The assurances were to be based on meaningful measures of successful and unsuccessful efforts to combat cybersecurity. The adopted voluntary mechanisms were:

1. Sector participation in FCC-initiated confidential company-specific meetings or other similar communications formats to share information;
2. Sector preparation of an annual sector cybersecurity report; and
3. Sector participation in Department of Homeland Security’s (DHS) Critical Infrastructure Cyber Community C3 Voluntary Program.

Barriers to implementation

The Requirements and Barriers to Implementation feeder group was tasked with considering what barriers exist that challenge the ability of communications companies to implement the NIST Framework. They also sought to elicit methods to overcome any barriers identified.

The first noted barrier to implementing cybersecurity measures was cost because any private company, regardless of its extensive use of the Framework, is unlikely to be able to withstand a concerted attack from a sophisticated nation-state attempting to breach its system. In addition, larger companies can be compromised through the thousands, sometimes tens of thousands, of interconnections they have with smaller players whose use of the Framework may be impractical to fully track.

The next noted barrier was the lack of legal protections regarding information sharing. Indeed, President Obama’s recent Executive Order called for information sharing among government, public, and private

sectors and encouraged a collaborative approach; however, there is still “uncertainty around information sharing." Indeed, the sub-team participants claim legislation that would support increased liability protections for information sharing would decrease uncertainty and allow for a more proactive approach to implementing better cybersecurity information sharing practices. Another barrier was technology.

Nature and trends of cybersecurity threats

The Threats Feeder Group was tasked to review the nature and trends of cybersecurity threats and investigate ongoing processes that could be used to gather, analyze, categorize, and share information about threats and vulnerabilities relevant to the telecommunications sector. In other words, best enable “threat informed” cyber risk management decisions.

As the sub-group noted:

> “Cyber thieves, industrial/political spies, and cyber-criminals often operate within a company’s own trust boundaries. Outbound threats are not always the result of an intentional attack. They often occur when an employee unintentionally opens a ‘back door’ by downloading a rogue application, opening an email attachment, or by clicking on a web link that could infect and possibly drop malware on the employee’s computer or edge device.”

As a result, they identified the most common types of Cyber Threats to Critical Infrastructure, in general, as:

- **Proprietary Espionage** – Targeted Information: Intellectual property; proprietary information; geopolitical, competitive or classified intelligence; etc.
- **Insider Trading Theft** – Targeted Information: Pending M&A deals or contracts; upcoming financial earnings; future IPO dates; etc.
- **Financial and Identify Theft** – Targeted Information: Employee and customer personally identifiable information; payment transactions; account numbers; financial credentials; etc.
- **Technical Espionage** – Targeted Information: Password or account credentials, source code, digital certificates; network and security configurations; cryptographic keys; authentication or access codes; etc.
- **Reconnaissance and Surveillance** – Targeted Information: System and workstation configurations; keystrokes; audio recordings; emails; screenshots; additional infection vectors; logs; cryptographic keys; etc.

The most common Attacker Target/Data Loss events in critical infrastructure systems the sub-group identified were:

- Account passwords and hashes, password filter installation, group policy modification
- Intellectual and sensitive property, regulated and classified data theft
- Confidential records, column-level encryption
- Corporate communications, business- and defense-related data, early warning of detection
- Infections from partner organizations and agencies

Consistent with other reports, including the 2014 Verizon Data Breach Report, the sub-group identified the

primary method for infecting targeted organizations as spear-phishing emails being sent to numerous targets. These phishing emails contain malware or malicious links to malware that exploits vulnerabilities found in popular operating systems, office applications, and programs. Attackers have successfully compromised organizations across every sector, including government and defense agencies, commercial enterprises, financial institutions, and scientific research facilities.

They issued six conclusions and recommendations:

1. **Continual Evolution –** The community threat models and threat intelligence handling models for threat awareness must continually evolve to respond to the ever changing tactics utilized by malicious actors and the unknown threats of tomorrow. Tailored threat knowledge can be used to better defend networks.
2. **Implementation of Agile and Adoptive Methods –** Current and future threat landscape will continue to evolve and will require agile and adaptive methods of obtaining threat intelligence, in order to adequately protect critical communications infrastructure.
3. **Threat Intelligence Gathering –** Organizations should continuously gather Threat Intelligence from a multitude of industry and government agencies, and cyber threat think-tanks to stay ahead of malicious actors and attackers and adequately protect critical communications infrastructure.
4. **Consider A Community Model –** A community model for threat intelligence or information sharing and analysis should be considered by organizations intending to use threat intelligence in their quest to protect critical infrastructure and protect critical data from future-unknown cyber threats.
5. **Leverage Threat Intelligence Capabilities –** Communications sector members should leverage the threat intelligence capabilities of the Communications ISAC (Comm-ISAC) as well as other intelligence sources, and consider participation in active and trusted community threat venues.
6. **Information Sharing –** Network operators within the communications sector share threat intelligence information with their peers (consistent with applicable laws), thus enabling more efficient and scalable threat information gathering for use in threat analyses and cyber risk management decision making.

The Telecommunications Industry Association applauds the work

The Telecommunications Industry Association (TIA), the leading association representing the manufacturers and suppliers of high-tech communications networks, applauded the CSRIC's adoption of cybersecurity risk management guidance and best practices.

TIA issued the following statement on March 18, 2015:

> "Today's adoption of the CSRIC's landmark report on cybersecurity risk management and best practices is a very important move towards improving cybersecurity for communications infrastructure. Importantly, it uses a voluntary, public-private partnership model to combat the complex cybersecurity threats our country faces in a dynamic and scalable way. TIA played an integral role in developing the CSRIC's recommendations. Voluntary collaboration between private and public stakeholders, rather than one-size-fits-all, top-down mandates, is essential to comprehensively evaluating and addressing evolving information security threats. We look forward to continuing to work with our partners in the next iteration of the CSRIC, and all stakeholders, to improve national cybersecurity."

”

Takeaways

The Report includes immediate and practical implementation guidance for the communications sector. Consistent with the NIST Cybersecurity Framework, it recommends that organizations implement a dedicated, organization-wide cybersecurity risk governance process. However, how each company implements such a cybersecurity risk management program will vary based on identified potential risk, risk tolerance, and other factors. For those companies in the five industry segments – broadcast, cable, satellite, wireless, and wireline – the Report includes an appendix for each one to suggest how cybersecurity risk management protocols and practices can be implemented.

For more information, please contact one of the attorneys listed below.

James J. Giszczak

Team member bio