Working Group 7: Legacy Network Best Practices Update

Status Update

March 20, 2014

Kyle Malady, Verizon, Chair

WG7 – Legacy Best Practices Update

Charter

WG7:

The majority of the best practices recommended by CSRIC address the reliability and resiliency of legacy communications networks, including 9-1-1 networks and services. CSRIC III took a fresh look at the 9-1-1 best practices, but the other legacy best practices have not been examined since CSRIC II. This Working Group will review the legacy best practices to identify where additional practices may be necessary given changes in technology, practices, or observed reliability trends. The Working Group will then recommend changes to the existing set of best practices to address the topics revealed by the foregoing analysis. Finally, the Working Group will consider revisions to best practices proposed by the Alliance for Telecommunications Industry Solutions and recommend how to incorporate these changes into the wider body of best practices.

Included Item:

Consider an issue related to security of manholes and expedited restoration following a associated outage.

WG7 – Legacy Best Practices Update

Current Objectives

March 2014:

✓ Consider an issue related to security of manholes and expedited restoration following a associated outage.

September 2014:

- Gap analysis of existing legacy best practices, identify where additional practices may be necessary given changes in technology, practices, or observed reliability trends.
- Recommend changes to the existing set of legacy best practices to address the topics revealed by the gap analysis process.
- Consider revisions to best practices proposed by the Alliance for Telecommunications Industry Solutions (ATIS) and recommend how to incorporate changes into the wider body of best practices.

March 2015:

- Recommend revisions to the best practice prioritizations based on CSRIC II WG6 recommended process.

CSRIC
Communications Security, Reliability and Interoperability Council

WG7 – Legacy Best Practices Update

Current Members (15)

WG-7 Member	Company
Kyle Malady (Chair)	Verizon
Mary Boyd	Intrado
Ron Boyer	Boyer Broadband
Tim Collier	Sprint-Nextel
Shahin (Shaw) Daneshkhah	Sprint-Nextel
Victor DeVito	AT&T
Stacy Hartman	CenturyLink
Robin Howard	Verizon
Rick Krock	Alcatel Lucent
John Marinho	CTIA
Bob Oenning	Earthlink
Andre Savage	Cox Communications
Andy Scott	NCTA
Gigi Smith	APCO
Kathy Whitbeck	Nsight

WG7 – Legacy Best Practices Update

Schedule & Status

- **Workload**
  - 476 Best Practices selected for evaluation
    - 275 Network Reliability, 176 Physical Security, 25 Disaster Recovery and Mutual Aid
- **Current Status**
  - 57% Best Practice reviews completed by subteams
    - Three proposed new, 13 proposed deletions, 283 modified, and three unchanged
    - Wording, Network Types, Industry Roles, and Keywords are majority of changes to be proposed in September 2014 Final Report.
    - Several Best Practices to be forwarded to Working Group 4 - Cyber Security Best Practices as out of scope for WG7
  - Best Practice Status review (e.g., Critical, Highly Important, Important)
    - In Progress

WG7 – Manhole Security

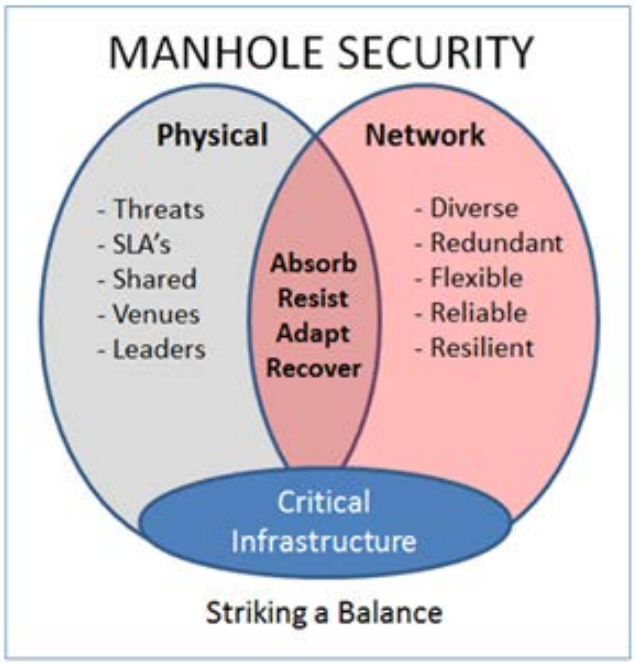
Executive Summary:

The Federal Communications Commission's (FCC) Public Safety and Homeland Security Bureau (PSHSB) requested that the Communications Security, Reliability and Interoperability Council's (CSRIC's) Working Group 7 – Legacy Best Practices Updates (WG7) consider an issue related to the security of manholes and how communications providers may be able to better expedite outage restoration following unapproved access and facility damage.

In the Interim Report, WG7 exams and provides useful information that will assist in better understanding this issue and the potential impacts on critical infrastructure physical security and resiliency. This report considers manholes used as part of the communication infrastructure with the primary concern of impacts on network reliability regardless of ownership. Finally, the report assesses ways that communication providers can expeditiously complete restoration requirements when events of this nature occur.

WG7 – Manhole Security

Key Points



Scope:

WG7 focused on security of manholes that are utilized by communications companies and did not contemplate other users of manholes.

- While this report focused on the issue of manhole security, it could as easily address the overall security of any outside plant component.
- How to strike a proper balance between physical security and daily operational access.
- Physically securing all of the nation's manholes is a complex project riddled with numerous issues including viable threat, vulnerability, and consequences.
- Physical security can deter intrusion into the manhole or vault, but the simple fact is that not all threats and vulnerabilities can be averted and intrusion events will happen.
- Through a combination of physical security, network management, and route resiliency a balance can be struck that broadens the range of protection options available.

CSRIC
Communications Security, Reliability and Interoperability Council

WG7 – Manhole Security

Strategy

Method	Advantages	Disadvantages
Physical Weight	• Difficult to lift without tools	• Tools readily available
Welding	• Cost effective and quick • No special tools to access • No keys to lose or misplace	• Tools for access readily available to non-authorized people • Increases access time
Paving Over	• Cost effective • Hides manhole from view	• Locating and access can be difficult if not impossible • Legitimate access time consuming • Emergency access is generally infeasible
Locking Devices	• Keyed for ease of access	• Keys can be lost or stolen • Rekeying covers not practical • Locking mechanisms can fail
Barrier Devices	• Keyed for ease of access • Pan sits under standard cover • Secures from below	• Keys can be lost or stolen • Rekeying covers not practical • Locking mechanisms can fail
Intrusion Alarms	• Timely notifications of entry • Remote surveillance • Situational awareness	• Cannot identify intent of access • Does not prevent access • Requires response procedures • Requires 24x7 alarm monitoring and response team
Surveillance (Video)	• Real time monitoring • Visual identification • Situational awareness	• Does not prevent access • Can be defeated • Requires response procedures • Requires 24x7 alarm monitoring and response team

Methods of Manhole Security

Network Strategy:

A strategy based on resilience fosters consideration of a broader range of options to help reduce the risks associated with the loss of critical infrastructure.

Physically Securing Manholes

- Each method has advantages and disadvantages which can unintentionally reduce network resiliency if the method precludes easy legitimate access when required.

Asset Protection

- Communication providers have an inherent incentive to protect their assets.
  - Ownership and Access
  - Underground to Aerial adds Network Vulnerabilities
  - Existing Federal, State, or Local laws
  - Customer Service Level Agreements (SLAs)
  - Real or Potential Threats and Special Manhole Security

Network Resiliency

- Communication and emergency services are more defensible and flexible when critical infrastructure is physically secured and selective diversity is implemented to provide resiliency.
  - Network Components (Reliability)
  - Route Diversity (Alternate Routes)
  - Detailed Plans for Recovery (Business Continuity)
  - Consumer Responsibility for Mission Critical Circuits

WG7 – Manhole Security

Conclusions

- When considering an outside plant intrusion scenario, whether related to manholes, utility poles, utility boxes, vaults, etc., similar security concerns exist.
- Securing some geographical portion of the millions of manholes across the country or even securing all of them still leaves the network vulnerable.
- It would generally be more coincidental that a mission critical circuit would happen to be on a damaged facility than for an act to transpire based on real knowledge.
- In the event of an act of intentional sabotage or terrorism, a determined person(s) would be likely to defeat any manhole cover security if the desire was strong enough.
- The most common method of securing manholes is through spot welding.
- Millions of manhole covers in place for decades have not experienced unauthorized access and/or vandalism. As such, these locations do not need to be further secured, unless a communications company becomes aware of a viable threat, issue or concern.

CSRIC
Communications Security, Reliability and Interoperability Council

WG7 – Manhole Security

Conclusions (Continued)

- There are situations and reasons that a subset of manholes should be further secured; however it should be up to the manhole owner to complete a risk analysis and determine which method is appropriate to utilize.

- In situations where law enforcement and/or internal security information identifies and presents a viable threat, cooperation by the manhole owner(s) is warranted and encouraged in order to protect our nation's critical infrastructure.

- In cases where non-communication utilities, consortiums, or municipalities operate the manholes that communication cables traverse, all parties should be encouraged to consider these security issues.

- In order to provide the highest level of critical infrastructure security, network resiliency is needed.

WG7 – Manhole Security

Recommendations

1. WG7 recommends that communication providers incorporate six current Best Practices as part of their resiliency design process for mission critical circuits where practical and feasible.
   - 9-7-0549, 9-7-5075, 9-7-5079, 9-7-1065, 9-8-0731, 9-9-5252

2. A new Best Practice recommendation that focuses on this issue. This Best Practice is associated with communication provider processes that at least one or more providers currently perform.

   Manhole Security: Network Operators and Property Managers should consider additional security measures for critical infrastructure utility vaults and manholes when presented with a viable threat or recommendation by law enforcement and/or internal security.

3. WG7 recommends that the CSRIC Council approve this report and the new Manhole Security Best Practice.

WG7 – Legacy Best Practices Update

Next Steps

- **Continue work on Best Practices by subteams**
- **Review ATIS NRSC recommendations on Best Practices from CSRIC III**
- **Review Best Practice Status definitions and prioritization**
- **Prepare Final Report for September 2014**