March 2014

WORKING GROUP 7
Legacy Best Practices Updates

Interim Report – Manhole Security

Table of Contents

1 Results in Brief

1.1 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. According to the PSHSB, this high priority issue evolved in the aftermath of several outages in 2013 and previous years and was directly related to vandals inappropriately accessing manholes and damaging communication facilities[1]. In this paper, WG7 will examine and provide useful information that will assist in better understanding this issue and the potential impacts on critical infrastructure physical security and resiliency. This paper considers manholes used as part of the communication infrastructure with the primary concern of impacts on network reliability regardless of ownership. Finally, the paper assesses ways that communication providers can expeditiously complete restoration requirements when events of this nature occur.

2 Introduction

As federal, state, local governments, and communication providers struggle with incidents of facility and equipment vandalism and theft our nation's vital communication fiber and copper cable infrastructure is threatened. This raises a fundamental question – about how to strike a proper balance between physical security and daily operational access. While this paper focuses on the issue of manhole security, it could as easily address the overall security of any outside plant component. These cables carry vital communications whether above or below ground. Mission critical circuits for consumers, government, and communication providers are generally aggregated throughout the countless miles of underground facility routes. These routes traverse the nation from densely populated urban areas down to the most rural of communities. For those

[1] Reference: "*Vandalism At San Jose PG&E Substation Called 'Sabotage,'*" at http://sanfrancisco.cbslocal.com/2013/04/16/gunshots-cause-oil-spill-at-san-jose-pge-substation/) last visited March 31, 2014.

bad actors that are determined to cause a disruption to communications or emergency services the unremarkable and often unobtrusive manhole cover is the equivalent of an unlocked door. On the surface, the most obvious response to securing manhole covers, is "to lock the doors" so to speak. However, when focusing singularly on this solution it becomes clear that physically securing all of the nation's manholes is a complex project riddled with numerous issues including viable threat, vulnerability, and consequences[2]. At the onset of any discussion of this nature it is common-sense to ask what it is that we are trying to accomplish. Are we trying to stop all unauthorized access to manholes? Or, are we trying to decrease risk to the communications critical infrastructure in the event an unauthorized intrusion event occurs? 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 (e.g., identifying and prioritizing high risk areas, securing manhole covers), network management, and route resiliency (which includes time and effort to restore operations and selectively utilize available diversity options) a balance can be struck that broadens the range of protection options available.

[2] Department of Homeland Security, *National Infrastructure Protection Plan*: Partnering to enhance protection and resiliency, 2009, p. 27.

2.1 CSRIC Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) IV									
CSRIC Steering Committee									
Chair or Co-Chairs: Working Group 1	Chair or Co-Chairs: Working Group 2	Chair or Co-Chairs: Working Group 3	Chair or Co-Chairs: Working Group 4	Chair or Co-Chairs: Working Group 5	Chair or Co-Chairs: Working Group 6	Chair or Co-Chairs: Working Group 7	Chair or Co-Chairs: Working Group 8	Chair or Co-Chairs: Working Group 9	Chair or Co-Chairs: Working Group 10
Working Group 1: Next Generation 911	Working Group 2: Wireless Emergency Alerts	Working Group 3: EAS	Working Group 4: Cybersecurity Best Practices Working	Working Group 5: Server-Based DDoS Attacks	Working Group 6: Long-Term Core Internet Protocol Improvements	Working Group 7: Legacy Best Practice Updates	Working Group 8: Submarine Cable Landing Sites	Working Group 9: Infrastructure Sharing During Emergencies	Working Group 10: CPE Powering

Table 1 - Working Group Structure

2.2 Working Group 7 Team Members

Working Group 7 consists of the members listed below.

Name	Company
Kyle Malady - Chair	Verizon
Mary Boyd	Intrado
Ron Boyer	Boyer Broadband
Tim Collier	Sprint
Shahin Daneshkhah	Sprint
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

Table 2 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

WG7's objective was to examine the issue of Manhole Security. To determine if there were existing Best Practices that applied and if so, whether they needed to be modified or if supplemental Best Practices are needed. WG7 also considered non-Best Practice recommendations that may be shared with other non-communication company manhole owners (e.g., utilities, consortiums, municipalities) addressing this security issue. Finally, the objective was to assess ways to mitigate unauthorized access to manholes and the effect of intrusions.

3.2 Scope

WG7 focused on security of manholes that are utilized by communications companies and did not contemplate other users of manholes. In light of the fact that these other users are not members of, or participants in the CSRIC (and not likely to adopt CSRIC Best Practices), we established that it would be appropriate to focus our efforts on communication industry participants. A review of the available subject matter could not quantify the total manholes dedicated to communication company infrastructure. However, our investigation established that a greater percentage of the nation's estimated 20-22 million manholes, although potentially critical in their own use (e.g., electrical, gas, transportation, sewer, or water), do not qualify under this study as communication critical infrastructure.

4 Analysis, Findings and Recommendations

4.1 Analysis

4.1.1 Physically Securing Manholes

Common methods used to physically secure a manhole can be as simple as through its own physical weight to more extreme methods such as welding, paving over, locking, or installing barrier devices. In some applications, security may take the form of alarming manhole access points in vaults that contain electronics or monitoring a video feed in a security center. We point out that there is a distinction between manholes that provide occasional access and those that provide access to electrified network elements that need more frequent access. Each of these methods has advantages, but also disadvantages which can unintentionally reduce network resiliency if the method used to secure the manhole precludes easy legitimate access when required. The table below illustrates the advantages and disadvantages of the most common methods used to secure manholes.

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

Table 3- Methods of Manhole Security

Cost and operational issues are substantial factors that must be evaluated in physically securing manhole access points. There are some means of securing a manhole that are relatively inexpensive such as the common practice of spot welding. This method secures the manhole but requires a more labor intensive effort to gain access and to re-secure the cover following any activity. Entry into a previously welded manhole requires only basic tools (e.g., hand grinder) which can be readily acquired even if one is not available at the onset of an event. Other manhole entry devices provide for more sophisticated securing and access; however under the right circumstances can, and have, caused considerable delay in restoration efforts. For example, some manhole covers utilize a keyed locking system which secures the cover to the enclosure. These keys are tightly controlled through limited availability to prevent unauthorized access to manholes. If a key is misplaced, lost, or stolen it can significantly delay access into the manhole during emergencies, maintenance or restoration efforts while a duplicate key is being located. If a key is stolen or a misplaced key is found by an unauthorized individual, a bad actor could readily gain access into any of the manholes the key is designed for. Over time locks can degrade or become contaminated making them inaccessible even with the correct key. Once security is breached, the ability to change the lock may be limited and may often be deemed impractical for the manhole owner. This keyed locking method is also used in barrier devices and is designed to fit just below the manhole cover also relying on repair crews to track and secure keys in between uses. Multiple key types may also be required to manage different manufacture types - further complicating the access and restoration processes. There are also more advanced manhole entry devices available that are made from composite materials (rather than metal). These can have built in security locks with the added benefit of eliminating any scrap value for potential thieves but have the same concerns with keys as other locking or barrier devices. It should also be noted that barrier devices can be potentially defeated from below if access can be gained through a tunnel, vault, or conduit from any non-

secured access point along the route. Intrusion alarms and video surveillance may offer an additional layer of security if available or coupled with other securing techniques; however, they still cannot prevent unauthorized access or potential intrusion threats.

4.1.2 Asset Protection

Communication providers have an inherent incentive to protect their assets and it is up to each provider to assess risk and determine how they will best secure those assets. There are a multitude of factors that must be considered when identifying the physical security options for manholes. One such factor is ownership of the various manholes, vaults, and/or ducts/tunnels the facilities go through along a route. Responsibility for managing the security and access of manholes range from private companies, including network providers, consortiums providing access to multiple entities, other utilities (e.g., power, gas, or water), or those publicly owned by state or local government entities. Critical circuits may traverse through several different underground routes that are owned by multiple entities that may provide various levels of security (if any). In densely populated cities where multiple utilities often share common routes, tunnels, or conduits there is also the issue of managing shared access to manholes. In some scenarios the manhole owner provides stringent procedures for requesting access and maintains full responsibility for opening and closing the access points. In other cases, the manhole owner may opt to contract out that task or provide unhindered and unsupervised access to tenants and other authorized personnel using their own internal processes. Cables can also leave the underground and go aerial at many different points along a route adding network vulnerabilities. Additionally, communication providers must consider any current federal, state or local laws pertaining to the securing of manholes as well as restrictions that may prevent physical security for safety reasons (e.g., OSHA regulations). Further, providers must consider Service Level Agreements (SLAs) entered into with their customers. The need to physically secure manholes may also be prompted by a real or potential threat brought to the attention of manhole owners by various law enforcement agencies or through their own internal security sources. In addition to communication security risks, large scale venue events and events where senior government leaders will travel along a planned route may warrant special manhole security as part of the event planning process regardless of any real risk or threat to communications. It is important to note that geographic topology or location may also negate the need for physical securing of a manhole. For example, there are many manholes that commonly fill with water when unattended and must be pumped out before access to cables can be made. Unauthorized access in these cases would be hazardous and difficult to accomplish due to the naturally occurring barrier. In addition to all the concerns mentioned above, there is an underlying cost for communication providers to police and manage manhole access that goes beyond physical security and adds another layer into the complexity of the issue.

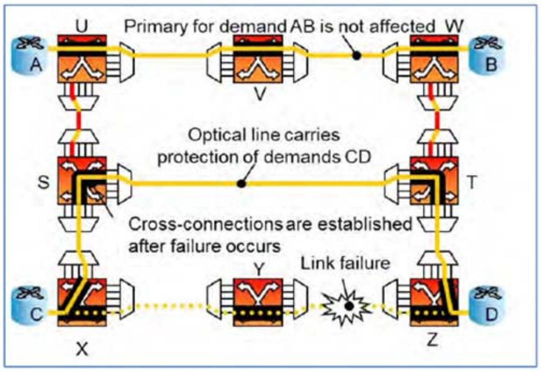
4.1.3 Network Resiliency

Communication and emergency services are more defensible when critical infrastructure is physically secured and selective diversity is implemented to provide resiliency. This strategy provides for a more flexible approach to the issue, limits potential impact to providers and consumers and provides for shorter restoration and recovery timeframes. One measure of network resiliency is the amount of time it takes to fully recover from an event and restore normal operations. The quicker the recovery, the more resilient the system will be.[3] In 2009, the *National Infrastructure Protection Plan* published by the Department of Homeland Security (DHS) defined resilience as "…the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions."[4] Risk is more fully diminished through redundancies in network components (reliability), route diversity designed by providers and their customers (alternate routes), and detailed plans for recovery as a result of an event (business continuity). Rather than singularly limiting access to the manholes where cables may traverse, communication providers should also consider designing mission critical circuits to include resiliency, which will make them far more protected and able to withstand deliberate damage. One method used to achieve resiliency is physical route diversity, which involves protection by designing one side of a critical circuit (working) to traverse over one unique route while the other side of the circuit (standby or protect) traverses over another unique non-intersecting distance separated route. In some cases this diversity is enhanced by continuous utilization of both routes making disruption of one virtually transparent to message delivery. Another method for

[3] Moteff, J. D. (2012, August 23). Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. Retrieved January 19, 2014, from FAS CRS: https://www.fas.org/sgp/crs/homesec/R42683.pdf

[4] Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009, p. 111.

attaining the same resiliency could be through the use of a mesh network architecture where a combination of protected and unprotected circuits are engineered in a way that allows traffic to self-heal around a damaged portion of the route as illustrated in Figure 1[5].



Shared backup path protection in a mesh architecture

Figure 1 – Mesh Architecture

Other methods that achieve resiliency may involve a combination of terrestrial and satellite, wireless and wireline, utilizing multiple providers, or consumers building a portion of the network themselves. The utilization of high capacity fiber network components along with protocols utilizing packet management dramatically increases diversity options. Regardless of the method(s) used to attain it, owners of critical circuits should periodically review recommendations outlined in existing industry Best Practices regarding diversity and apply them to the extent practicable and/or feasible for their business.

Consumers should also consider their responsibility in ensuring their mission critical circuits are designed with resiliency in mind. In February 2006, the Alliance for Telecommunications Industry Solutions (ATIS) published the National Diversity Assurance Initiative (NDAI)[6] to "provide customers with the knowledge they need to identify the diversity risks that exist in their current telecommunications environment. It also provided them with terminology that could be used to establish a common understanding with carriers when evaluating circuits for diversity assessment and assurance, as well as how circuits are engineered to address diversity concerns. Customers could then better determine the acceptable level of risk as it pertains to their

[5] http://en.wikipedia.org/wiki/File:SBPP-after_failure_and_recovery.jpg
[6] ATIS-I-0000041, *National Diversity Assurance Initiative*, February 2006, Page 16.

telecommunications services." As well, a January 2006 report by the Critical Infrastructure Task Force of the Homeland Security Council concluded that a strategy based on resilience would foster consideration of a broader range of options to help reduce the risks associated with the loss of critical infrastructure. The Task Force did not suggest that resilience replace protection efforts, but that resilience offered an overarching strategy that included protection, preparedness, and efforts to prevent attacks from happening.[7] These customer efforts at assuring diversity appropriate to their application should be ongoing in recognition that technologies evolve.

[7] Homeland Security Advisory Council. *Report of the Critical Infrastructure Task Force*. January 2006.

4.2 Findings

WG7's research into this issue found several existing documents discussing recommendations for the securing of manhole covers. Some limited their recommendations and focused on installing special locking devices on manhole covers in and *around* facilities[8], while others suggested that a combination of statutory requirements, fund allocations, and tax and insurance credits be applied to a tiered geographic implementation and noted that this approach was the "most practical, effective, and affordable means to protect these underground assets."[9] Another document adopted a resolution that supported the securing of nine million manholes in the nation's metropolitan and urban areas through federal policy, study and funding to secure our cities' vulnerable underground infrastructure by protecting it against breaches of our most critical manholes.[10] These documents, which we found insightful, focused singularly on physical manhole security but did not address an equally critical component of this issue; which is limiting potential impact through the use of network resiliency.

[8] Joint DHS and FBI Information Bulletin, Title: *Potential Threat to Homeland Using Heavy Transport Vehicles*, Date: July 30, 2004, page 6 of 7.

[9] *Manhole Security, Protecting America's Critical Underground Infrastructure*, Irwin M. Pikus, PH.D., J.D., November 2006, page 17.

[10] The United States Conference of Mayors, 2007 Adopted Resolutions Criminal and Social Justice, Protecting City Critical Assets Underground Infrastructure and Manhole Security.

4.3 Recommendations

As outlined in Figure 2, in order to strike a manhole security balance, one side must consider the need to provide physical security from known threats, recognize customer Service Level Agreement (SLA) requirements, identify shared manhole access points, and respond to large venue events and government leader protection issues. As well, providing selective facility route diversity, component redundancy, flexible technologies, reliable network elements, and an overall resilient network must be taken into consideration. When these components are in balance, the network is better prepared to absorb, resist, adapt, and speedily recover from a manhole security related event.

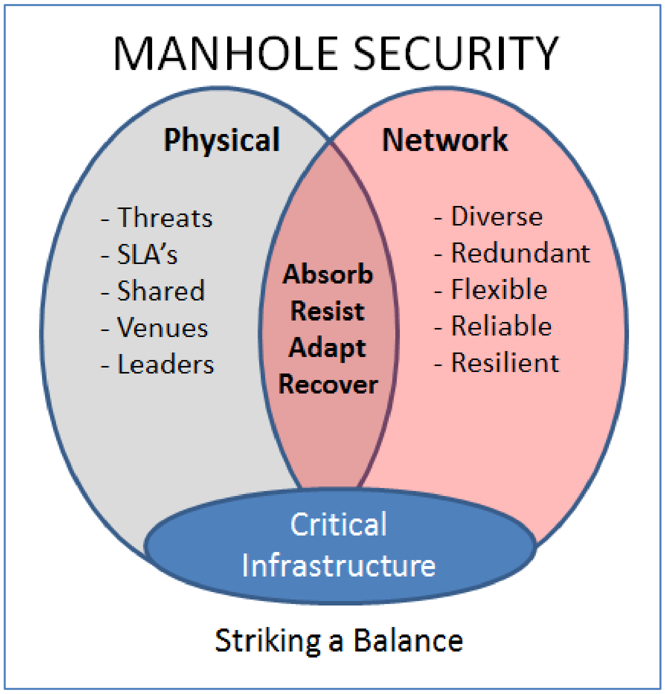


Figure 2 – Physical and Network

WG7 identified current Industry Best Practices that address network diversity and resiliency as discussed in this Interim Report which are provided in the table below. WG7 recommends that communication providers incorporate these Best Practices as part of their resiliency design process for mission critical circuits where practical and feasible.

NUMBER	BEST PRACTICE
9-7-0549	Network Operators should develop an engineering design for critical network elements and inter-office facilities that addresses diversity, and utilize management systems to provision, track and maintain that inter-office and intra-office diversity.
9-7-5075	Network Diversity: Network Operators and Service Providers should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path).
9-7-5079	Network Operators and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links (e.g., nodal, network element). Particular attention should be paid to telecom hotels and other concentration points.
9-7-1065	Network Operators and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and subscriber services considering security, functional redundancy and geographical diversity.
9-8-0731	Network Operators and Service Providers should provide physical diversity on critical inter-office and wireless backhaul routes when justified by a risk or value analysis.
9-9-5252	Network Operators should evaluate the priority on re-establishing diversity of facility entry points (e.g., copper or fiber conduit, network interfaces for entrance facilities) during the restoration process.

Table 4- Diversity Best Practices

Appendix 1 outlines 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. WG7 also recommends that the CSRIC Council approve this report and the new Manhole Security Best Practice.

WG7 also recommends that the FCC consider a future CSRIC Working Group charter item to contact non-communication sectors to determine if current Best Practices exist in these sectors that could be applied to the communication sector regarding the issue of Manhole Security.

5 Conclusions

WG7 carefully evaluated the issue of manhole security from a number of perspectives. In consideration of recent intrusion events, the team took a real-world look at the issue. When considering an outside plant intrusion scenario, whether related to manholes, utility poles, utility boxes, vaults, etc., we found that similar security concerns exist. In fact, securing some geographical portion of the millions of manholes across the country or even securing all of them still leaves the network vulnerable. Various methods of routing underground and aerial cables are widely used to routinely carry mission critical circuits, both in urban and rural geographical settings. WG7 also considered the issue of how an intruder would know with any accuracy or certainty what traffic is riding any given route. It seemed that 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 (unless some type of insider information had been shared). It was rationalized that 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. Based on this and common industry practice, WG7 determined that the most common method of securing manholes is through spot welding. It has proven to be effective where justified and limits unauthorized access while not incurring the potential issues associated with other keyed security measures. WG7 concluded that millions of manhole covers have been in place for decades that 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. WG7 further agreed that 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. WG7 also concluded that in order to provide the highest level of critical infrastructure security, network resiliency is needed. As discussed earlier, communication providers and their end user customers must collaboratively work to design and implement a level of network resiliency that appropriately balances physical security, network resiliency, and cost benefit.

6 Appendix 1 – Best Practices

Recommendations for Best Practices:

Working Group 7 - Legacy Best Practices Updates recommends the following Best Practice to address the issue of Manhole Security.

CSRIC IV Best Practice Number	CSRIC IV Best Practice	CSRIC IV BP Reference/Comments	Best Practice Status	CSRIC IV (New/Changed/ Unchanged/ Deleted)
BEST PRACTICES NEW				
WG7-1-1	**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.	**Network Types(s):** Cable; Internet/Data; Wireless; Wireline **Industry Role(s):** Network Operator; Property Manager **Keywords(s):** Access Control; Buildings; Transport Facilities; Network Design; Physical Security Management **Remark(s):** Facilities requested to be secured by public safety should be considered critical.	Highly Important	**New**