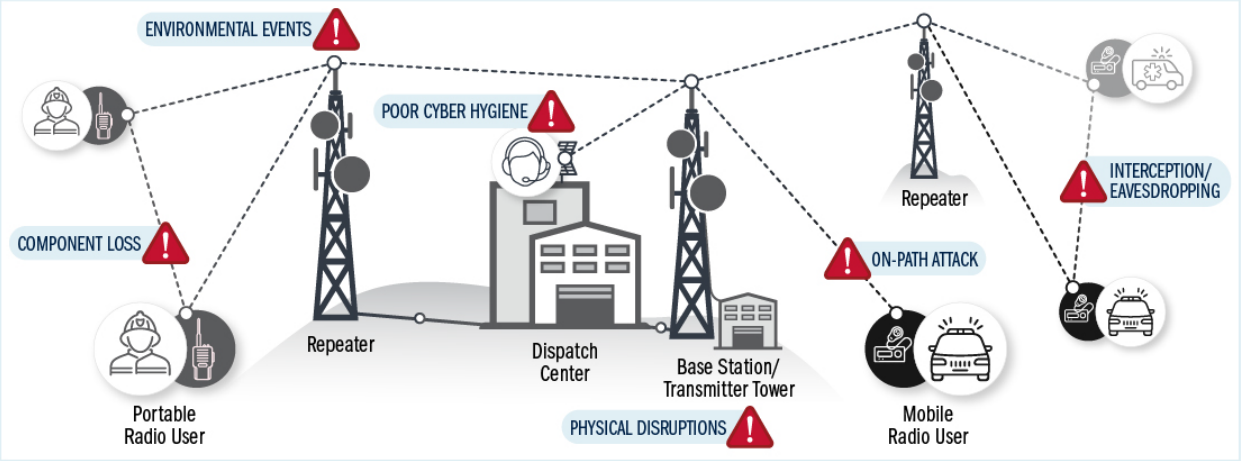
Compliance Testing LLC | 1724 S. Nevada Way | Mesa, AZ 85204 |

www.ComplianceTesting.com | www.p25testing.com |480-748-4449

LMR Cyber Security Assessment and Remediation

LMR Systems

Land Mobile Radio (LMR) systems are designed to provide instant, reliable, and secure mission-critical push-to-talk communications to the public safety and first responder community. However, the digitizing of LMR systems has made their networks, devices, and data susceptible to cyber threats.



Cyber Risks

Cyber risks manifest when a cyber attacker or cybercriminal gains unauthorized access to a network, device, or data and affects the confidentiality, integrity, or availability of the system or information. Some consider LMR networks closed systems that are not exposed to cyberattacks and do not see cybersecurity as an important component of their LMR system. However, LMR systems are vulnerable to multiple cyber risks that could negatively affect critical communications.

LMR System Vulnerabilities

LMR systems are terrestrially based, wireless communications systems commonly used by federal, state, local, tribal, and territorial first responders, public works companies, and the military in tactical and non-tactical environments.

Supporting voice and low-speed data communications, LMR systems typically consist of handheld portable radios, in-vehicle mobile radios, base stations, and repeaters. A network ties the components together.

- **Handheld portable radios** - carried by operations personnel and tend to have a limited transmission range.
- **Mobile radios** - located in vehicles and use the vehicle's power supply and a larger antenna, providing a greater transmission range than handheld portable radios.
- **Base station radios** - in fixed locations, such as emergency communication centers (ECCs), public safety answering points (PSAPs), or dispatch centers, and tend to have the most powerful transmitters
- **Repeaters** - increase the effective communications range of handheld portable radios, mobile radios, and base station radios by retransmitting received radio signals.
- **Network** - connects LMR system components, serves as a transport mechanism for voice and data communications, and extends the communications coverage area of the LMR system. In addition to the LMR system components, LMR networks contain servers, routers, microwave systems, and in some cases, interface with public IP networks to increase the reach or coverage of the communications system and improve interoperability.

LMR systems are vulnerable to compromises such as encryption hacks, disruptions to the physical infrastructure, and jamming. Agencies are implementing emerging wireless broadband services and applications. When broadband applications are enabled to meet mission-critical voice applications, many public safety agencies may migrate to broadband voice applications to augment voice LMR systems to form a "converged network."

Are you looking for assistance in risk evaluation and mitigation for your LMR systems? Objectives of the Compliance Testing LLC Cyber Security Program:

- Identify vulnerabilities in the radio communication infrastructure and the devices used by emergency responders.
- Develop an action plan for remediation.

A detailed plan can be built using the following steps.

1. Define the scope.
2. Set testing schedule.
3. Develop test cases.
4. Execute the test.
5. Analyze the results.
6. Create a remediation plan.
7. Implement the remediation plan.
8. Test again.
9. Monitor and report.

LMR Systems Penetration Test Program

Define the scope: Identify the specific LMR systems and devices that will be tested, including the radio communication infrastructure and the devices used by emergency responders. This should include both the hardware and software components of the systems.

Set testing schedule: Determine how often the testing will be conducted, taking into account the organization's risk profile and regulatory requirements. It's recommended to conduct testing at least once a year.

Develop test cases: Create detailed test cases that describe the testing methodology, tools, and techniques that will be used during the test. This should include testing for vulnerabilities in the radio communication infrastructure and the devices used by emergency responders.

Execute the test: Conduct the testing using the test cases developed in the previous step. This should include both manual testing and automated tools.

Analyze the results: Review the findings of the test and identify any vulnerabilities that were found. Determine the potential impact of those vulnerabilities on the organization and prioritize which vulnerabilities should be addressed first.

Create a remediation plan: Develop a plan to address the vulnerabilities that were identified, including prioritizing which vulnerabilities should be fixed first and determining the resources needed to fix them.

Implement the remediation plan: Take the necessary steps to address the vulnerabilities that were identified, such as applying software patches, configuring security controls, or updating policies and procedures.

Test again: Once the vulnerabilities have been addressed, conduct another penetration test to confirm that the remediation efforts were successful and that the LMR systems are now more secure.

Monitor and report: Monitor the LMR systems for any new vulnerabilities, and report any issues found to the appropriate parties.

Key Client Questions

1. What type of communication and data transfer requirements does your municipality have for your radio network, and how do these requirements impact your overall cybersecurity posture?
2. Have you experienced any security incidents or challenges related to your radio network, and if so, how did you address them?
3. How do you currently manage and monitor the security of your radio network, and what tools and processes do you have in place?
4. How do you ensure the physical security and integrity of your radio infrastructure, such as base stations and radio equipment?
5. What measures does your municipality take to ensure the security of the equipment and components throughout the supply chain for your radio network?
6. How does your organization ensure that your radio network uses strong, up-to-date encryption protocols to secure data transmission?
7. Can you describe your current approach to monitoring your radio network for potential cyber threats, and how effective has it been in detecting and preventing incidents?
8. How do you ensure that the firmware on your radio equipment is up-to-date and free of known vulnerabilities?
9. Can you describe the current network segmentation in place for your radio network, and how does it help to limit the potential spread of an attack or compromise?
10. What measures do you take to ensure the security of the equipment and components throughout the supply chain for your radio network?
11. How do you identify and manage potential insider threats to your radio network, and what safeguards are in place to protect sensitive information and systems?
12. Describe the physical security measures in place to protect your radio infrastructure, such as base stations and radio equipment.
13. Do you have a block diagram or component listing of your radio system?

How Can We Get Started to Help You?

1. Schedule a Teams meeting with our engineering/cyber security team.
2. We will discuss your system:
3. Identify your concerns and priorities. What is most important to you in both the long and short term.
4. Brainstorm a path forward (“next steps”).
5. Our engineering team will then use this information to develop a comprehensive “custom test plan” to meet your objectives.
6. We will present the custom test plan, and scale it to your main interests and budget needs.
7. Our team will plan all aspects of the project and oversee the execution to your complete satisfaction.
8. We will provide detailed documentation of test results and recommendations to address any issues identified.

For additional information please see:

https://www.cisa.gov/sites/default/files/publications/22_0906_safecom_cyber_risks_to_lmr_first_edition_v2_508C.pdf