NG-911 Cybersecurity

A Starting Point

From a County Viewpoint

February 2020

There are a few grounds rules to understand about cybersecurity.

1) There is no such thing as a “fully” secure network, assuming there are users, and the devices are plugged in.
2) Cybersecurity is a journey not a destination.
3) You cannot protect what you do not know about.
4) If you do not monitor and audit the devices, networks and logs, you have no idea what is really going on.
5) If you say “you have never had a security incidence”, it is because you do not know that you have had a security incidence.
6) Cybersecurity is not an afterthought, it needs to be baked into all process from the beginning.
7) You cannot just purchase a service or device and magically be protected.
8) You cannot ignore risk, you must manage risk.

Inventory is critical! This is not just about physical inventory, software inventory is just as important. You need to know what makes up the network and what version of hardware, firmware and software you have. You need to have very detailed network diagram(s) that must include any and all configurations, as well as, connections inside and outside of your environment. You will not achieve proper network cyber security with a single device or vender. Security needs to be layered and managed.

Policies, plans and auditing is vital to a successful outcome. At this time it appears there is very little of this being done in MN as it relates to the NG-911 systems and networks operating at each PSAP. Due to the critical nature of 911 we need to start with some “low hanging fruit” as soon as possible. To accomplish this requires that we 1st look at our own 911 systems and networks at our individual agencies. In the past when this has been attempted the vender(s) push back and do not want to give counties access to “their 911 network”, or any real configuration information. This needs to change. Some of the very critical issues that are not too hard to analyze are:

Detailed list of hardware with support and end of life status.

Detailed list of all software with current patch levels.

Detailed local network diagrams.

Detailed configurations of Switches, Firewalls and Routers.

Collection of logs and a review / monitoring process.

Start of a process to create the 1st layer of security policies and auditing processes.

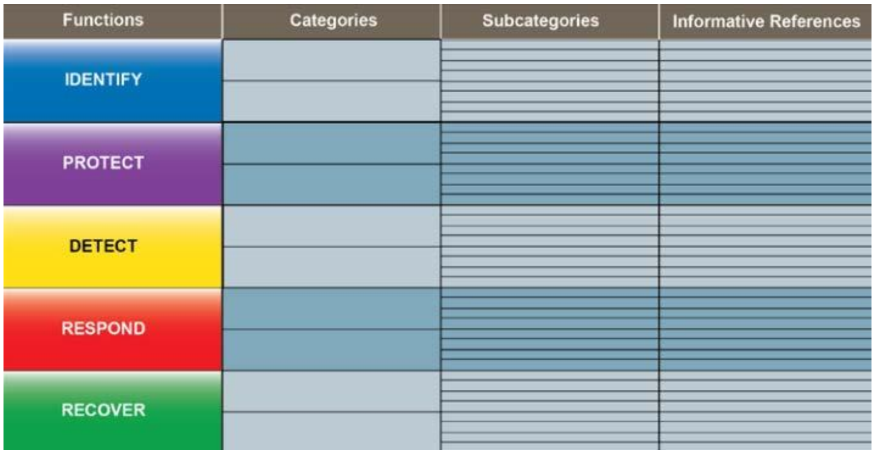
Starting an iterative process to deal with the issues as they are discovered i.e. risk management.

Improving NG911 Cybersecurity Posture

Given the dynamic nature of technology and the evolving cyber risk landscape, organizations should adopt a cybersecurity framework. An effective framework enables response organizations to:

- *Identify new and evolving risks*
- *Assess and prioritize risks*
- *Develop and prioritize mitigation strategies based on cost-benefit analysis and other factors*
- *Evaluate the impacts of mitigation implementation*
- *Develop an approach to detection and effective response and recovery procedures*

The Department of Homeland Security (DHS) strongly recommends adopting the NIST Cybersecurity Framework, which is a flexible, risk- based approach to improving the security of critical infrastructure.5 Collaboratively developed between government and the private sector, the framework is based on industry standards and best practices and can be used for NG911 systems. The NIST Cybersecurity Framework is designed to complement an existing cybersecurity risk management process or to develop a credible program if one does not exist. Figure 4 demonstrates the five core tenets of the NIST Framework: identify, protect, detect, respond, and recover. More information, including informative reference for addressing each tenet can be found in the NIST Framework.



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

(Credit to DHS NG911 Cybersecurity Primer)

The most recent NIST Cybersecurity Framework and related newsletters are available at: http://www.nist.gov/cyberframework/.