SPECS SURVEY: Mics and Mobile Radio Antennas | WHAT'S NEW: Digital Radio

RadioResource

September-October 2018 | MCCmag.com

MissionCritical™

COMMUNICATIONS

Cybersecurity in Public-Safety Communications

Inside

TETRA Radio Service and Maintenance

Emergency Communications During California Wildfires

Cybersecurity in Public-Safety Communications

Changing communications technology requires public safety to be constantly vigilant when it comes to cybersecurity issues. **By Neil Horden**

While the topic of cybersecurity for public-safety communications systems is popular with the industry press and conference presentations, agencies are taking little protective action. The predominant attitude among stakeholders is that cybersecurity is something to address in the future; unfortunately, that future is now.

There is a gaping disconnect between the awareness of the potential problems that cyberattacks can cause and the relatively little action being taken to prevent them. Understanding what caused this significant gap is a complex question with several critical components.

One problem appears to be overconfidence in the security of existing systems. The industry has operated sophisticated technology-driven systems for years with an excellent record of avoiding cyberattacks. The trunked radio and E9-1-1 systems that create the core of public-safety communications used cutting-edge technology when they were first developed. If any environment could have been an early and easy target for hacking, it would have been these systems. However, the way the systems were built and connected, the cost of computing power, and the relative immaturity of the hacker environment protected them.

Only recently have significant issues started to arise. Some problems can be attributed to the greater activity of hackers looking to exploit vulnerable systems of all types for profit or notoriety. However, the majority is attributable to the fact that current technology systems are more susceptible to cyberattacks.

Almost every facet of the critical public-safety communications system has changed, and almost all of the changes have opened the systems to cyberattacks. From the hardware and software on which networks operate to the interconnection of networks to the greater dependence on shared resources, systems are no longer capable of avoiding cyberattacks.

In an environment where the status quo is perceived as "good enough," action will only be taken when decision-makers understand the importance of taking cybersecurity seriously and acting immediately. This requires understanding how each change has weakened the overall structure of once nearly impenetrable systems. The systems have changed in three basic areas:

- Legacy systems were built on proprietary hardware and software, but today's systems are built on open standard hardware and software.
- Legacy systems were connected with point-to-point links (RS-232/485 and/or T-1 links), carrying mostly proprietary protocols. Current systems are almost exclusively designed around

Ethernet connections using open transmission control protocol/IP (TCP/IP).

■ Legacy systems operated on primarily closed networks, but systems now are more open and interconnected.

Future systems will continue to evolve in the direction of standardization and openness, further increasing these risks.

Standardized Operating Platform Risks

Past-generation radio systems had relatively few computing and software components. When trunking was introduced, it was primarily based on proprietary hardware systems running proprietary operating systems. An adversary would have to design an attack for the specific system, which is seldom seen. The level of effort would be quite high and the potential return quite low, giving these systems a near-zero risk of cyberattack.

As systems have evolved, so has the computing industry. While proprietary hardware and software were required in the past, the power and flexibility of new computing platforms provides a better solution with significant benefits. Standardized hardware provides greater levels of processing power at reduced costs. Additionally, standardization brings a wealth of development tools, greatly reducing the effort to design a complex system.

Even though cybersecurity is often considered a component of each system, to be truly effective, it must be considered comprehensively and coherently across all systems.

Current generation systems are almost entirely based on industry-standard computing platforms. The combination of standardized operating systems and software, combined with standardized hardware, is the norm for almost all computing systems. The advantages of this architecture are significant, from the availability of greater levels of data processing power at lower costs to access to a rich set of development and testing tools. The enhancements in reliability and redundancy cannot be understated. Even the current migration to virtualized platforms, with its many benefits, is because of the use of industry-standardized operating system platforms.

However, along with the benefits come a large number of potential hacking risks. As systems become standardized, the number of systems susceptible to the same type of attack — often called an attack vector — increases, not only allowing an adversary to design an attack usable on a

large number of systems, but an attack designed for another system could be inadvertently or purposely released onto your system. People using USB drives infected from other systems and technicians connecting infected laptop computers caused some of the first cybersecurity issues encountered in public-safety systems.

Unfortunately, with this migration, essentially every attack vector that any computing platform can experience becomes a threat. As public-safety systems come to have more in common with the rest of the consumer and commercial computing world, they also become susceptible to the many cyber-attack vectors targeting those systems. This issue increases the risks two ways. Systems become susceptible to the broad-based attacks targeting standardized platforms, and hacker tools are readily available to adversaries, making targeted attacks on public-safety systems a significant risk. Those responsible for these systems should not underestimate the broad availability of these tools to a greater base of potential adversaries.

Fortunately, the mainstream computing industry is working to address many of these issues. Software providers quickly supply fixes of various types — patches, system updates and anti-virus/anti-malware programs — as they find threat vectors capable of infecting any significant number of system implementations. However, the level of vigilance required to maintain updated protection from these ever-evolving threats is often overlooked. Many agencies fall short in addressing these known cybersecurity risks, leaving systems open to attack.

Interconnection Technology Evolution

The transition started with IP links, followed by standardized IP protocols. As with hardware and software, interconnection technology has aligned public-safety networks with the technology of commercial and consumer networks.

Legacy public-safety communications systems used few digital interconnecting links. Even when digital links started being used, most were based on either serial formats common to industrial computer systems of the time or T-carrier formats common to the telecommunications industry. In both cases, these links operated primarily in a point-to-point architecture and were difficult to hack without making a physical "tap" or midpoint connection. Additionally, because much of the data transferred used proprietary protocols, general cyberthreats were uncommon.

This changed with the adoption of IP technologies. The near-universal adoption of the standardized set of IPs for packet networks has provided a wealth of benefits for communications systems, including ease of providing reliable and redundant routing of information between components, sharing data and equipment between various functions to provide significantly greater system efficiency, and

ease of connecting systems from multiple vendors — not to mention the cost efficiencies of standardized routing routines, replacing expensive proprietary protocol stacks and the availability of standardized management tools.

Of course, the use of IP packet networking aligns public-safety communications systems with the greater IT networking market and again opens systems to the many cybersecurity risks common to the IT world. As with the computing platform risks, routing architecture risks are addressed by IT vendors through their continuous development of preventative measures. This again cannot be a "set-and-forget" environment. It takes vigilant attention to network cybersecurity to make sure a network is appropriately protected. The easy mistake is to assume that the network is still closed, but most every network becomes more open.

The use of IP technology is often not seen as a significant issue within public safety because the interconnection networks supporting these communications systems have traditionally been closed, single-purpose systems. These networks were believed to be secure because it would typically take a physical connection to monitor or attack the system. These systems typically existed primarily within secure facilities, and the risk of a physical connection was considered low. However, the cybersecurity issue is real as most networks have migrated from closed to open.

The closed network concept runs counter to standardization and interconnection trends.

Network opening occurs both inadvertently and intentionally. Inadvertent opening of the network occurs when the ease of IP networking allows the unintentional creation of paths to the internet through other systems that touch the network or the failure to restore proper firewall setting after diagnostics and servicing. While inadvertent network connections are often addressed through training and careful control of network access points, intentional network connections are often a bigger issue.

Intentional connections are created when the previously closed network requires access to external resources, such as for emailing trouble reports or giving network access to an external

user. The functions and benefits of IP networking created this risk and allow it to grow. Features such as remote monitoring evolve from being mere conveniences that can be discontinued for security reasons to hard requirements that must be secured without limiting functionality.

Often virtual private networks (VPNs) and firewalls are used to create a mixed open/closed network to support the desired operation. The application of a VPN and the use of firewalls can be an effective part of network security, but they do not stand alone. Both measures require active monitoring and management to maintain their effectiveness as barriers to a cyberattack. VPNs are often disabled, and firewalls have excess ports opened as temporary measures during troubleshooting and as temporary fixes to network problems. These short-term and temporary actions are commonly left undocumented and uncorrected for long periods of time, leaving a system susceptible to cyberattack. The only resolution is vigilant attention to cybersecurity and an ongoing process of monitoring, testing and protecting the network.

Open Networks

Public-safety communications systems have become more interlinked, and connection to systems operating on other agency networks is increasing. Next-generation 9-1-1 (NG 9-1-1), shared CAD resources and integrated data applications drive this emerging requirement.

External connections to external networks are no longer accidental or occasional occurrences. They are now critical design requirements that provide mandatory functions. As systems continue to evolve, interoperability and interconnection of networks are increasing. The use of the Inter RF Subsystem Interface (ISSI) to interconnect Project 25 (P25) networks and similar intersystem links often travel over external, internet-connected networks. The interconnection of public-safety networks will only continue to expand. In addition, the even less controllable requirements to interface with cellular, the First Responder Network Authority (FirstNet) and other nontraditional networks are increasing. All of these connections add to the potential for a cybersecurity attack.

Jurisdictionwide shared networks have become common. The same factors affecting public-safety radio systems now occur on the dispatch side of systems. Previously secure public-safety answering point (PSAP) systems are harder to keep safe. Core applications such as call-taking, CAD and records management have moved to industry-standard commuting platforms and operating systems. Additionally, much as interoperability is driving interconnection on the radio side, NG 9-1-1 is driving interconnection between agencies and jurisdictions on the dispatch and PSAP side, often requiring direct internet access to enable needed functionality.

The only resolution is vigilant attention to cybersecurity and an ongoing process of monitoring, testing and protecting the network.

As changes occur within public-safety communications systems, they are also occurring across the IT world. The concept of a closed or dedicated network runs counter to the trends of standardization and interconnection. The migration from purpose-built networks to shared networks creates a world where the network is perceived as a utility for the entire agency or jurisdiction. Dedicated and closed networks are a thing of the past that public safety cannot fall back on for cybersecurity protection.

What Public Safety Must Do

Public safety must put as much attention into cybersecurity requirements as it puts into other system requirements. There are processes to define, implement and maintain radio, dispatch and IT systems. These same processes need to be applied to the definition, implementation and ongoing maintenance of the cybersecurity aspects of all three. Just as it takes a level of expertise to properly ensure that each system meets its defined requirements throughout its operational life, public safety must make sure that it applies the same level of expertise in cybersecurity.

Even though cybersecurity is often considered a component of each system, it must be considered comprehensively and coherently across all systems to be truly effective. For this reason, it is often beneficial to manage cybersecurity requirements above and outside each individual system with the resulting criteria being applied to each system in a cohesive manner. Once applied, the support of these cybersecurity requirements must be embedded into the ongoing monitoring, maintenance and upgrade processes on these systems. Even the training programs must include cybersecurity as a core component.

Cybersecurity can no longer be an afterthought layered onto the network. It must be more than just something reviewed periodically to keep up. It must become an actively developed and managed part of the network. It must become a mission-critical requirement of the overall organization, to the same level as the communications systems it protects. ■

Neil Horden has more than 34 years of experience in wireless communications working with manufacturers and users in the LMR and carrier markets. As chief consultant for Federal Engineering, he is responsible for the technical oversight of the programs. He is on the editorial advisory board of *MissionCritical Communications* magazine, and is a board member of the Project 25 Technology Interest Group (PTIG) and the NG9-1-1 Institute. Email comments to editor@RRMediaGroup.com.