Securing Your Next-Gen Network

As public-safety agencies transition to broadband and data in the cloud, they encounter new security and privacy challenges.

By Greg Shine

Two important developments that are improving emergency communications are also effectively mandating a transition to next-generation systems for public-safety agencies. The first is next-generation 9-1-1 (NG 9-1-1) and the second is the First Responder Network Authority (FirstNet), the nationwide network dedicated to public safety.

Moving to next-generation technology eliminates many of the communications challenges that existed when agencies and first responders used different frequency bands. Using mobile tools, emergency medical technicians, firefighters and police officers can access rich sources of information ranging from real-time location data, high-resolution images from closed-circuit television (CCTV) or video surveillance footage from drones, all helping them gain greater understanding of the risks in whatever scenario they may be facing.

Mobile technology puts vital information into the hands of public-safety responders when they need it most. In high-pressure emergency situations, the ability to access rich sources of real-time data improves situational awareness, enhances communications and knowledge sharing between agencies, and increases the speed of decision-making when time is a critical factor.

Communications Transformation

The transformation to next-generation technology is coming, so public-safety communications managers and decision-makers who have not already started putting a strategy in place need to do so sooner rather than later. A critical part of this strategy must involve protection and control to ensure data is secure at all times.

Having a well-defined approach to security and privacy that protects all connected devices, together with data at rest and in transit are key parts of demonstrating communications maturity. As agencies begin to build a mobile ecosystem, they need

to protect their end users in the face of cyber threats while staying compliant with state and federal security and privacy regulations. This article provides a five-point checklist that can give your agency's next-generation technology strategy a solid grounding.

This approach is necessary because although next-generation technology brings many benefits, the connected world brings risks for first responders. In-vehicle and on-person connected devices have become critical pieces of equipment in police cars, ambulances and fire trucks. There have been examples of body cameras being vulnerable to hacking, which makes it possible for criminals to tamper with or delete video evidence. There is also a present risk of offensive cyber activity by nation-state attackers.

Ransomware infections have also increased, and there have been rising numbers of attacks seen across the nation from Albany, New York, to Riviera Beach, Florida, to South Carolina to California. Ransomware attacks pose a twofold threat to public-sector agencies, severely disrupting operations and hindering responders' ability to fulfill their missions. The nature of ransomware means that attackers gain access to victims' personal data. This presents a privacy risk because first responders may be accessing criminal records or patient details.

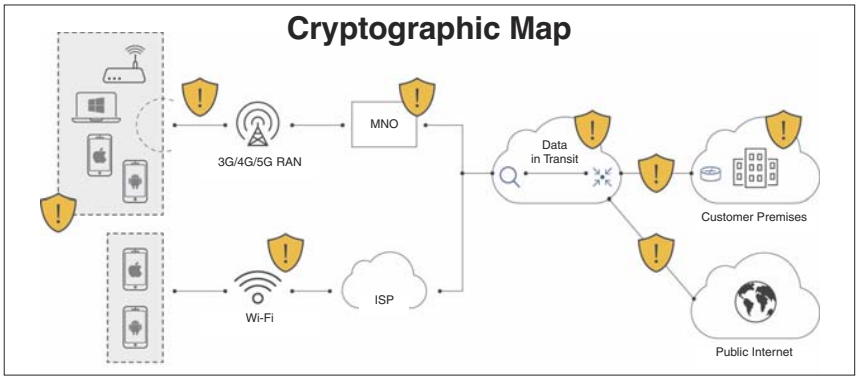
The Mobile Ecosystem

To understand the security and privacy implications, let's look at the typical mobile ecosystem in more detail. A public-safety agency will likely have a variety of assets at its disposal to assist in missions, including wearable technology such as body cameras and firefighters' smart suits, along with ruggedized tablets, in-patrol car routers and first responder smartphones.

Using those tools, agencies access a variety of different data sources that may be hosted on the cloud or on premise. Many agencies still maintain their own servers back at base, which they connect to remotely. In the line of duty, responders may also need to access state or federal services such as hospital data, vehicle records or state criminal records that may be cloud side.

When officers and first responders are in the field, they may not be able to access a Wi-Fi network, so they will use cellular access to connect to these systems over the internet. It's a hybrid environment, so they can't just use a virtual private network (VPN) to protect the data while it is in transit.

By standardizing on subscriber identity module (SIM)-enabled devices, public-safety agencies can create fully secure tunnels that protect not only the hardware but the data. This gives communications managers full visibility and control over their entire mobile ecosystem,



Organizations need to ensure strong end-to-end data encryption and security.

helping public safety meet its regulatory compliance obligations under Federal Information Processing Standards (FIPS) 140-2 and Criminal Justice Information Services (CJIS). It also addresses the privacy-by-design demands that are fast arriving. As various states pass legislation based on the California Consumer Privacy Act template, public-safety agencies must ensure they're protecting the data they hold on devices and while it's being transmitted to or from cloud systems.

Communications managers at public-safety agencies must deliver a secure internet experience to first responders by protecting and managing their endpoint devices to avoid the risk of infection with malicious code. If a device does become infected, IT administrators should be able to quickly identify rogue behavior and isolate the source to prevent further spread.

Pillars of Security

The cybersecurity field provides a useful approach to protecting data with a framework based on three pillars: confidentiality, integrity and availability. Using these principles as a guide ensures data is kept safe only for those authorized to access it (confidentiality), data can't be tampered with or compromised (integrity), and data is accessible and online at all times (availability).

Informed by these principles, agencies can start to formulate a next-generation technology safety strategy with five parts:

1. Humans continue to be a potential weak point in the cyber chain, either through being targeted by hackers directly or by their own unwitting actions such as using easily guessed passwords or opening files with a malicious payload. No matter the size of an organization, one of the best investments is to continuously educate your first responders about the benefits and the risks they're exposed to. Provide training courses that explain the security

issues and test afterwards to ensure they have absorbed the lessons.

2. Formulate policies in employee handbooks that clearly outline what users can and cannot do on their devices, such as looking at social media during work hours. This reinforces the messages in your training.

3. Deploy technologies for management, visibility and control of the mobile ecosystem appropriate to the size of your organization and the resources available to it. For larger agencies, the technology could be security incident event management (SIEM) tools and mobile threat defense that provide visibility over the entire mobile device estate to rapidly detect possible indicators of compromise. For smaller agencies, consider technologies that are easier to roll out, such as unified endpoint management tools to manage mobile devices combined with network layer mobile data protection and management services. Also, ensure that the devices you select are protected.

4. You must encrypt and secure data in transit from all points. When choosing a networking and communications solution, carry out due diligence to ensure any suppliers you intend to work with can demonstrate certified compliance with the relevant standards, including FIPS and CJIS.

5. Agencies must also protect data while it is at rest. Choose the correct mobile SIM-enabled devices fit for purpose from accredited vendors and ensure the suppliers' technologies are FirstNet certified. You can also enhance the devices with complementary mobile device management (MDM) or unified endpoint management (UEM) software to provide additional protection.

In addition to the above guidelines, FirstNet also provides an approved and certified listing of suppliers of hardware and software that it recommends public-safety agencies source from.

Recently, the National 911 program released a self-assessment tool for administrators in emergency communications centers and public-safety answering points/emergency communications centers (PSAPs/ECCs) to help administrators evaluate a system's maturity state ahead of adopting NG 9-1-1 at 911.gov. Together with the five-point checklist outlined previously, your agency can gain the appropriate levels of security, protection, visibility, compliance and control. This ensures the transition to next-generation technology brings all of the benefits while managing and mitigating the risks. ■

As head of security and compliance, Greg Shine manages the information security function in Asavie with the sole mission of keeping Asavie and its customers' data safe. Shine's previous roles in banking, finance and payments with IBM, Lloyds TSB and First Data International give him a strong security background, which helps Asavie maintain a vigilant security posture. Email feedback to editor@RRMediaGroup.com.