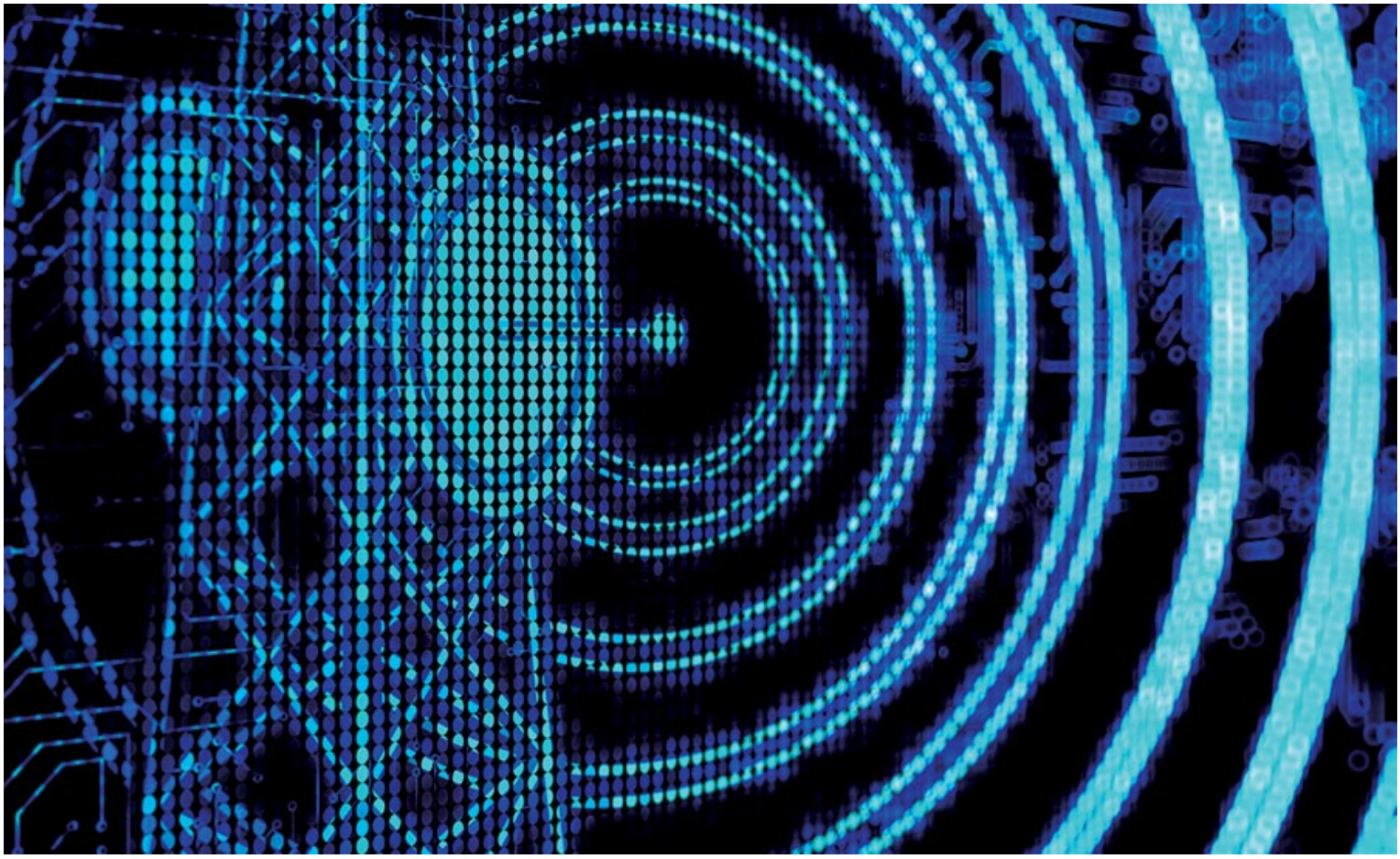
SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

Six reasons radios are unable to support today's security teams



November 30, 2020

Gregory P. Taylor

Today's physical security teams contend with modern-day threats that create risks for the people, property, and brand identities they protect.

Executive security is increasingly complex and dynamic. A pre-COVID-19 study in Harvard Business Review found that CEOs spend less than 50% of their time at headquarters. They spend the rest of their time in dynamic security environments, including other company visits, commuting, and travel. Coordinated terrorist efforts on social media are a growing threat as well. The recent kidnapping plot against Michigan's Gov. Whitmer only emphasizes how social media can facilitate the transformation of an online threat into physical criminal activity. Real-time threats raise the bar for real-time collaboration solutions to ensure safety and compliance.

Patrols need better tools to protect physical property more effectively. Security teams involved in property and asset protection need technology to better manage risks, including dynamic identity management, protocol compliance, and urgent or emergency incident responses.

Physical security is also increasingly entwined with protecting intellectual property or company data. IBM estimates that 10% of today's data breaches are driven by physical security compromises and cost an average of $4.4 million per breach.

Innovation and digital transformation should be priorities for enterprise-wide security operations in the face of today's threat environment. Today's bad-actors have access to contemporary technology, necessitating security teams to be on-par and adopt faster, smarter technology that amplifies their ability to do their jobs safely and effectively.

Too often though, decision-makers overlook the strategic value and potential in replacing outdated radios that severely limit real-time collaboration and emergency preparedness. In truth, security teams can no longer rely on the radio technology that hasn't changed since the 1990s.

These six reasons demonstrate compelling evidence that radios are ill-equipped to provide today's security teams with the situational intelligence they need in a high-tech world:

Reason No. 1: Dynamic field communications

Radios are obsolete. Today, the regulated spectrum and two-way radios are an old-fashioned concept not suited for responding to dynamic incidents involving the protection of people and property.

Security teams need multimodal communication platforms that offer voice, text, and visual media on one secure platform and provide the crucial information that improves their effectiveness. A multimodal collaboration tool provides quick voice updates, offers real-time information to support dynamic incident response, and captures data for more accurate incident reporting.

Multimodal collaboration enables security teams to create a complete picture of a dynamic incident and respond efficiently as a coordinated unit.

Reason No. 2: Unified response

Radios are deficient in range and functionality. Today's security teams need modern technology that facilitates infinite possibilities of 1:1, group, and mass communications — at any time, no matter the location.

Frequently, security teams rely on one set of radios to communicate with each other and phones or even alternate radio systems to communicate with people outside their groups. The lack of range and interoperability for radio systems means that security teams may have to go through other people and multiple devices to reach the right contact. In emergencies, this slows down response time.

Let’s take one example of a property manager with multiple sites and multiple security teams. A threat enters Site One but quickly moves to Site Two before being apprehended. Due to the poor range of radios, the two properties have different radio systems that are incompatible and work on different frequencies.

The two teams are unable to coordinate a unified response. They must relay information first to their team on their radio system and then to the other site by second device or phone and back again. Security guards on Site One cannot immediately communicate with security guards on Site Two without intermediaries who are likely communicating with their team by radio and the alternate site by phone — a significant waste of time and resources in an urgent situation. If the police are involved, this adds another set of radios and another set of contacts to be coordinated by phone or alternate device.

With a contemporary collaboration service, the property management organization can create unlimited team or 1:1 groups to enable direct connections, eliminating the need to use phones. During emergencies, security teams should have one device that can connect with anyone they need to communicate with on the fly and not be locked down by range or which radio network or frequency their device can access.

Smart collaboration tools that run on phones or devices powered by LTE (including 5G and private LTE), mesh, Wi-Fi, or satellite enable users to add someone to a new group immediately — regardless of which party owns the service. This also means that if incidents occur while a manager is offsite, they can receive an immediate alert and communicate with their teams instantly.

Reason No. 3: Dynamic and urgent situation support

Unlike radios, today’s technology facilitates process automation to increase a security teams’ safety and effectiveness in dynamic situations.

Process automation offers infinite possibilities for workflows that provide advanced situational intelligence in incidents like a man-down or urgent threat. Automated processes support the security team's event response by immediately kicking off a predefined procedure or workflow.

In the case of a man-down alert, a voice-activated trigger such as saying “help-help” can begin a procedure that starts with alerting management, identifying the location of an incident, and relocating team members to assist.

Radios are limited to voice-only communications, but intelligent bots and workflows are always on, listening and instantly acting to provide added resources to boost the safety and effectiveness of urgent situations.

Reason No. 4: Advanced location services

Radios lack screens and maps. They are limited to providing two-way communications, but advanced geolocation information provides precise GPS mapping, fleet tracking, or checkpoint verification. Security teams need this geolocation intelligence to immediately know where their team members are located with precision — key for emergency response and reaction to dynamic incidents.

Executive protection offers a prime example of how advanced geolocation reinvents collaboration for security teams. A security team leaves a geofenced workplace with an executive en route to a second location. Geofenced triggers and fleet tracking then start workflows that prepare each member of a security team at the new site to receive the executive.

In the predesigned workflow, the second security team can be alerted by the geofenced trigger as soon as the executive leaves the workplace, monitor where the executive is by GPS, and know when the executive enters the new geofenced site in order to prepare the new location for the arrival of the executive — all without anyone ever having to manually take an action to provide updates. Instead, the security team can stay present and focused on keeping the executive safe.

Reason No. 5: Reduce repetitive and routine tasks

Radios are unable to support automation. High turnover and low employee engagement plague the security industry. Low pay and minimal benefits can lead to turnover as high as 300 percent a year for some companies. Security teams staffed by a revolving suite of employees with minimal training can make even secure places vulnerable.

Like many deskless workers, security teams are subject to performing routine tasks that can take up a significant portion of their day, every day. These repetitive tasks include incident reports, protocol compliance, checklists, or dynamic identity management, which all require onboarding that most teams don’t have time for.

The good news is that 80% of security leaders believe digital transformation will deliver significant non-financial benefits, such as enhanced employee experience and greater engagement. Digital transformation offers enormous ROI and reinvents how security teams operate. By replacing radios with technology that automates processes, rookie team members become experts in following protocols from Day One.

Reason No. 6: Analytics

Radios lack the ability to store, track, and analyze a security team’s activities. The big data from smart collaboration tools provides critical situational intelligence and analytics capabilities that simply aren’t available with radios. One hundred percent of an organization’s message stream and real-time geolocation data provides advanced situational analysis that transforms how security teams respond to evolving events, manage routine tasks, and evaluate activities to improve performance.

Unlike radios, smart tools offer endless opportunities to improve security. Managers need to know where their guards are and how long they've been there, and team members need intelligence and support that enhances their productivity. For instance, pattern analysis can identify when guards linger too long in one place, if two team members' coverage areas overlap, or if there is a coverage gap.

Today's security teams need process automation to chart and improve surveillance paths and ensure complete and randomized surveillance. This technology increases the effectiveness of a security team and their strategic pattern analysis.

The solution

Ultimately, radios require significant investment but offer limited return on value. They are holding enterprise security operations back and adding unnecessary risk to the security teams. Designed a century ago, radios are limited to two-way communication and have failed to evolve to meet today's multimodal, intelligent standards and best practices.

Security teams need more than just the voice-only communication of radios. True collaboration tools provide operational command and control, process and workflow automation, intelligence amplification for team members, and analytics to inform best practices. With all this, collaboration technology can transform security teams with better productivity, safety, and engagement.

Security teams need technology that is as advanced as the threats they face. They need a voice-first intelligent collaboration platform that empowers them to do their jobs better.

Gregory P. Taylor is Chief Executive Officer at Orion Labs, a voice-first, intelligent platform.