

BEYOND WI-FI: THE WIRELESS READINESS GAP IN MODERN BUILDINGS

MODERN BUILDINGS CAN HAVE EXCELLENT WI-FI AND STILL FAIL TO PROVIDE THE CELLULAR CONNECTIVITY, MOBILITY, RESILIENCE, AND OPERATIONAL COMMUNICATIONS THEIR OCCUPANTS AND SYSTEMS INCREASINGLY DEPEND ON.



Paul Weintraub
RCDD, RTPM, ESS, TECH

General Director
Excigent

paul@excigent.com



THE WIRELESS READINESS GAP

“The building has Wi-Fi. So why do people still lose signal?”

It is a simple question, but it exposes an increasingly important issue in modern building design. People often treat wireless connectivity as synonymous with Wi-Fi. Yet users do not think in terms of network layers. They expect phones to work, applications to authenticate, messages and calls go through, and mobile services to remain available as they move throughout a building. A facility can therefore have excellent Wi-Fi and still have significant wireless gaps.

The problem often starts with the building itself. Materials that improve energy efficiency, structural performance, and security — such as low-emissivity glass, concrete, and structural steel — can also block radio-frequency propagation. Dense interior construction and below-grade spaces further weaken

signals from outside the building, and elevators, stairwells, parking structures, mechanical rooms, and deep interior spaces are frequent trouble spots.

This creates a wireless readiness gap: the building appears connected because Wi-Fi is available, even as reliable cellular service and other communications needs go unaddressed.

WI-FI AND CELLULAR DO DIFFERENT JOBS

Wi-Fi remains essential — it supports enterprise LAN access, guest connectivity, collaboration, managed devices, and many local and IoT applications. But it is only one layer.

Public cellular provides native voice, messaging, and mobile data without requiring users to join the building's network. That matters for visitors, customers,



Orlando Calderon

Sales Engineer for
the Caribbean, Latin
America, and Canada
Nextivity

ocalderon@nextivityinc.com

contractors, and employees using personal devices, as well as for mobile applications, multifactor authentication, cloud services, and other workflows that depend on carrier connectivity.

Reliable in-building cellular also supports mobility as users move through offices, corridors, elevators, parking structures, and interior spaces where outdoor cellular signals may not penetrate consistently.

Private LTE or 5G can support dedicated operational, industrial, campus, or other controlled applications, while IoT networks handle sensors, automation, and monitoring. In many buildings, these technologies complement each other.

The design question, then, should not be “Which wireless technology should we install?” It should be “What does the building need to support?”

PUBLIC WI-FI IS NOT THE SAME AS TRUSTED CONNECTIVITY

Reliable cellular coverage matters for another reason: users should not assume a public Wi-Fi network is trustworthy simply because its name looks familiar or because a hotel, airport, conference venue, restaurant, or other public location offers it.

When cellular service is weak, people may join unfamiliar Wi-Fi networks, use public hotspots, or accept whatever connectivity is available — behavior that can increase cybersecurity exposure.

A hotel Wi-Fi phishing campaign reported in

August 2026* showed how compromised Wi-Fi gateway infrastructure and manipulated DNS settings could redirect travelers trying to reach legitimate Microsoft services to fraudulent Microsoft 365 sign-in pages. To the user, the connection could appear normal while attackers targeted credentials or authentication tokens.

The broader lesson is that connectivity and cybersecurity cannot be treated as separate conversations.

A properly designed public or private cellular network can provide a separately managed communications path that does not depend on the building's local Wi-Fi infrastructure. Cellular is not immune to cybersecurity risk, but reliable indoor cellular gives users another connectivity option when Wi-Fi is unavailable, impaired, or untrusted.

In a changing environment where threats, devices, network conditions, and user behavior cannot all be controlled, maintaining more than one viable communications path improves resilience.

The In-Building Wireless Ecosystem

A complete strategy may include multiple layers



Image: The in-building wireless ecosystem. A complete strategy may include multiple layers.
Source: Paul Weintraub *RCDD, RTPM, ESS, TECH* / Orlando Calderon

PUBLIC SAFETY IS A SEPARATE REQUIREMENT

Evaluate emergency responder communications separately from commercial cellular and enterprise Wi-Fi. Requirements may vary by country, jurisdiction, and facility, and difficult areas such as stairwells, parking structures, basements, and other interior spaces may require particular attention. Strong Wi-Fi or commercial cellular coverage should not automatically be assumed to satisfy emergency communications requirements. Public-safety communications are a distinct design consideration.

COVERAGE IS ONLY THE BEGINNING

Signal strength alone does not define wireless performance. A more useful framework considers four factors:

- 1 COVERAGE:**
Can users connect where they need to?
- 2 CAPACITY:**
Can the system support the expected number of users and devices?
- 3 RELIABILITY:**
Does performance remain consistent over time?
- 4 RESILIENCE:**
Can important communications continue when normal systems or conditions are disrupted?

A smartphone may show acceptable signal strength while the network still struggles under high density, performs inconsistently in critical areas, or lacks an alternate communications path.

START WITH THE REQUIREMENT, NOT THE PRODUCT

Before selecting an in-building wireless solution, owners, consultants, and integrators should first understand the environment. Consider building size and layout, construction materials, indoor and outdoor signal levels, known dead zones, user density, device types, carrier expectations, operational systems, IoT applications, and future changes. Evaluate public cellular coverage—and, where appropriate, private cellular—alongside Wi-Fi.

Only then should you consider deployment models. Depending on the facility, the approach may include Wi-Fi optimization, cellular signal extension, distributed antenna systems, small cells, private wireless, or a hybrid architecture.

A hospital, office tower, warehouse, hotel, and data center may require different approaches. But in many facilities, in-building cellular is the missing layer even when Wi-Fi is strong.

Modern buildings increasingly depend on wireless communications as essential infrastructure. The objective is no longer simply to “get a signal,” but to provide the right connectivity for the right application, in the right place, when it is needed.

Wi-Fi connects users to the building’s network. In-building cellular helps keep them connected to the outside world. Modern buildings increasingly need both.

That is the difference between having Wi-Fi and being wirelessly ready.

Sobre los Autores:

Paul is an ICT leader with over 30 years driving broadband, data centers, connectivity, and network automation across the Americas, EMEA, and APAC. A seasoned Fiber Connect speaker, he helps global organizations align technology strategy, smart infrastructure planning, hybrid cabling deployment, and strong commercial execution.

Orlando is a telecom and RF professional with over 30 years leading wireless design, optimization, and technical sales across the Americas and Europe. At Nextivity, he solves complex in-building coverage, capacity, and connectivity challenges for enterprise, commercial, and mission-critical environments with proven strategic focus.