Avaya Nexus Consumer Survey Report:
The Human Psychology of Critical Communications Infrastructure

Representative Survey of U.S. Consumers | April 2026

"When your life, your money, or your health is on the line, what do you expect from the phone system on the other end?"

Introduction

In April 2026, Avaya fielded a national consumer survey to answer a question the industry has been debating for years — but has never asked the public directly:

The answers were not ambiguous. They were a mandate.

We surveyed 509 U.S. consumers — census-weighted, employed full-time, spanning every major region and demographic group — and what emerged was not a set of preferences. It was a set of non-negotiable demands that redefined how enterprises must think about voice infrastructure.

We learned that:

- 82% say crystal-clear, instant voice connectivity with essential services is very important or higher — even in an AI-powered world.
- 65% say only a crystal-clear human voice makes them feel secure during a financial or medical crisis. Chatbots score 14%.
- 88% are concerned that banks and hospitals will replace dedicated phone systems with video conferencing technology. Only 6% welcome the idea.
- 89% say a single communication failure erodes their trust. 12% say it completely destroys trust.

This is not a story about nostalgia for the telephone. It is a story about infrastructure — and the gap between what consumers demand and what most organizations have built.

Every survey question in this report was designed to move beyond opinion and into consequence: what happens to trust, to safety, to clinical accuracy, to brand reputation, and to institutional liability when voice infrastructure fails? The data maps directly to the decisions that CIOs, boards, and technology leaders face today — and the consumers have already rendered their verdict.

Each finding will be unpacked not as raw data but as a signal—an early indicator of a permanent shift in how consumers evaluate the institutions they depend on. From transactional to trust-building. From best-effort to mission-critical. From collaboration-platform telephony to purpose-built voice infrastructure.

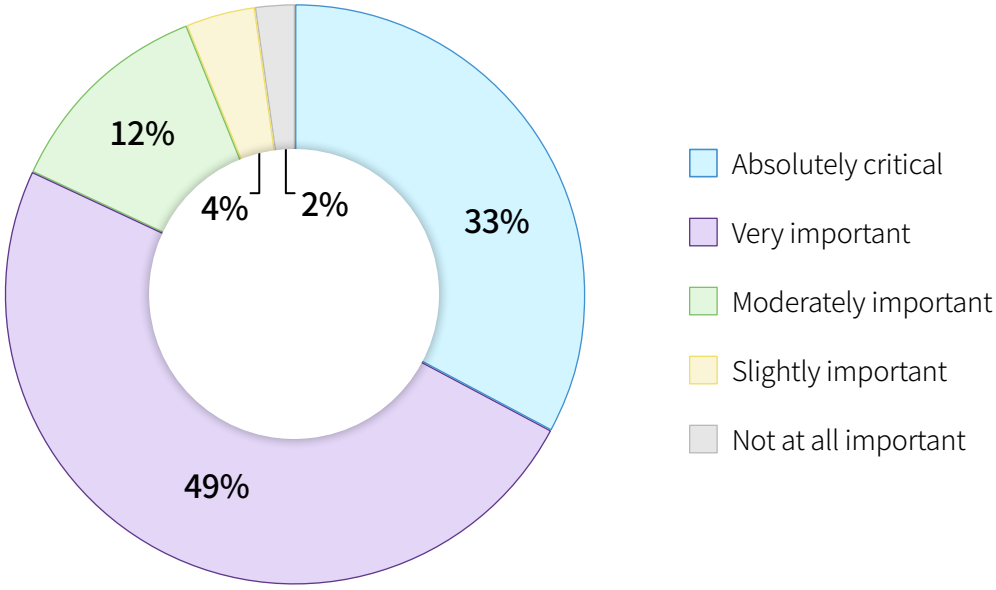
The consumer has drawn a line. This report shows you exactly where it is.

Welcome to the mandate for critical communications infrastructure
The voice connection is the trust connection.

1: The Non-Negotiable Call — Why Crystal-Clear Voice Is the Baseline

Question:

When you contact a healthcare provider, bank, utility company, or emergency service by phone, how important is it that the call connects instantly with crystal-clear audio?



Key Insight

A resounding 82% of U.S. consumers say crystal-clear, instant voice connectivity with essential services is very important or higher — signaling that, even in an AI-powered world, reliable voice infrastructure remains non-negotiable.

What It Means for Businesses

Technology has transformed how people connect with brands. But when it comes to critical moments — a medical question, a fraud alert, a utility outage — people still demand voice.

Consumers aren't asking for perfection. They're demanding excellence. The plurality at "Very important" (49%) signals pragmatism: they understand that systems aren't flawless, but they still expect their healthcare provider, bank, or utility company to deliver a voice that is always on, always clear, and always reliable. The 33% who rate it "Absolutely critical" leave no room for ambiguity.

Any platform that cannot guarantee this level of performance is operating below what four out of five consumers consider acceptable. This is the starting line, not the finish line.

- Empathy, not just efficiency, becomes the true differentiator.
- Human interaction isn't a fallback — it's a feature that builds confidence and care.
- Critical communications infrastructure must go beyond self-service to deliver emotionally intelligent experiences that start with being heard.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Brands can differentiate by engineering communications experiences that start with reliability, clarity, and always-on availability. AI can enhance, but not replace, the foundational voice layer that consumers demand.

Risk:

- Over-automation or AI-only service models risk alienating consumers at their most critical moments. Organizations that fail to invest in carrier-grade voice infrastructure risk falling short of the baseline expectations held by 82% of the public.

Action:

- Use AI to prepare human agents with full context and history — so they can respond quickly and with emotional intelligence.
- Invest in infrastructure that delivers deterministic, high-fidelity voice—not best-effort quality layered on general-purpose platforms.
- Ensure escalation to a live agent is always available, fast, and seamless, with a crystal-clear connection.

Final Thought

Human agents are no longer just troubleshooters — they're trust-builders. In today's critical communications environments, the agent becomes the bridge between what a customer feels and what a brand stands for. But the agent can only deliver that trust if the infrastructure beneath them is flawless.

Why You Need Avaya Nexus

Framing the Experience:

This research confirms the foundational shift: consumers judge institutions by the quality and reliability of their voice infrastructure. The most successful organizations are those that:

- Engineer voice systems for zero-downtime reliability
- Blend AI speed with human care on high-fidelity connections
- Deliver resolution with clarity and emotional resonance

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees the voice connection as more than a utility — it is a trust signal, a competence signal, and a brand signal.
- With Avaya Nexus™, organizations can deliver the full story of their commitment — not just the current ticket, but the assurance that the infrastructure will never fail when it matters most.

How the Data Maps to Important Shifts

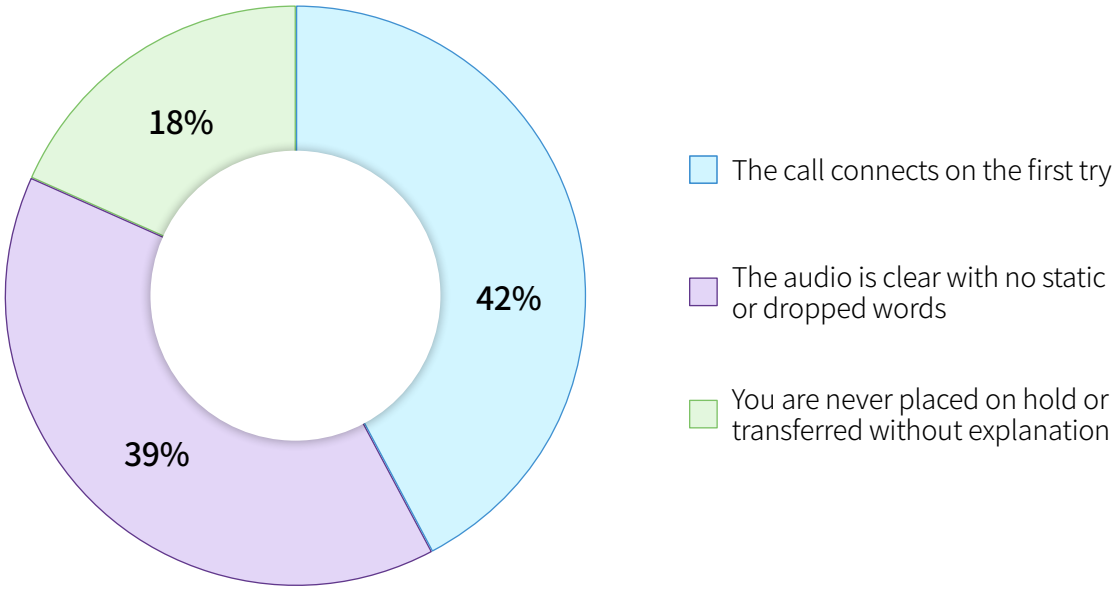
From	To
Best-effort voice quality	Carrier-grade, deterministic voice
Collaboration-platform telephony	Purpose-built critical communications infrastructure
Voice as a cost center	Voice as a trusted asset
Hoping the call connects	Engineering zero-downtime connectivity

Takeaway for the C-Suite

This is more than a service preference — it's an infrastructure mandate. 82% of consumers hold essential service providers to the highest standard for voice connectivity. Brands that invest in purpose-built, mission-critical voice infrastructure — and deliver both reliability and clarity at scale — will win trust, loyalty, and confidence. Those who don't will lose all three.

2: The Forced Priority — Consumers Refuse to Choose Between Reliability and Quality

Question:
If you had to choose just one, which matters most when calling an essential service?



Key Insight

When forced to choose, 4 in 10 consumers say the #1 priority is that the call connects on the first try — and nearly as many demand perfect audio. The combined 81% for connection reliability and audio quality means consumers refuse to separate the two. They want both, and they penalize the absence of either.

What It Means for Businesses

The near-even split between connectivity (42%) and audio clarity (39%) tells a stronger story than a single dominant winner. It tells decision-makers that consumers treat reliability and quality as inseparable dimensions of the same expectation. A platform that delivers crystal-clear audio but drops calls is failing. A platform that connects every time but delivers garbled sound is also failing.

This is the infrastructure challenge that general-purpose platforms were never designed to solve. Collaboration suites prioritize feature breadth — video, chat, messaging, file sharing — while treating voice as one more commodity feature in the bundle. But when 81% of consumers say that connection reliability and audio clarity are the only things that matter, the feature-breadth argument collapses.

- Connection reliability and audio quality are coequal consumer demands. Sacrificing one for the other fails on both counts.
- Hold-time management, while important, is a distant third — consumers solve the reliability and quality problem first.
- Infrastructure decisions must treat first-attempt connectivity and high-fidelity audio as non-negotiable, simultaneous requirements.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that deliver both instant connectivity and flawless audio on every call create a competitive moat that feature-rich but unreliable platforms cannot match.

Risk:

- Platforms that sacrifice voice reliability or audio quality to optimize for cost, feature count, or deployment simplicity will fail to meet the standard set by 81% of consumers.

Action:

- Deploy carrier-grade SIP routing engineered for first-attempt connectivity — not consumer-grade telephony bolted onto a collaboration suite.
- Invest in high-fidelity, wideband audio infrastructure that preserves voice clarity across every connection.
- Architect for both simultaneously — Dual-Availability Zone deployment ensures the call connects, and high-fidelity voice engineering ensures it sounds right.

Final Thought

Consumers are telling us something the procurement spreadsheet can't: reliability and quality aren't line items to be traded off. They are the twin pillars of trust. Every infrastructure decision that compromises one to save on the other is a decision to operate below the standard that 81% of consumers demand.

Why You Need Avaya Nexus

Framing the Experience:

This data validates the Avaya Nexus™ dual promise: instant connectivity and crystal-clear audio are not features to be selected — they are the architecture itself. The most successful critical communications environments are those that:

- Equip every connection with carrier-grade routing for first-attempt success
- Deliver high-fidelity audio that preserves clarity and emotional nuance
- Refuse to trade reliability for convenience or cost

Empowering the Critical Communications Mindset:

- A mission-critical mindset doesn't choose between reliability and quality. It demands both as foundational.
- With Avaya Nexus™, organizations don't make trade-offs — the Dual-AZ architecture and next-generation session services deliver both, every time.

How the Data Maps to Experience Shifts

From	To
Choosing between reliability and quality	Demanding both as non-negotiable
Feature breadth as the buying criterion	Voice reliability as the buying criterion
Hold-time optimization is the top priority	First-attempt connectivity as the top priority
Best-effort telephony	Carrier-grade, purpose-built voice

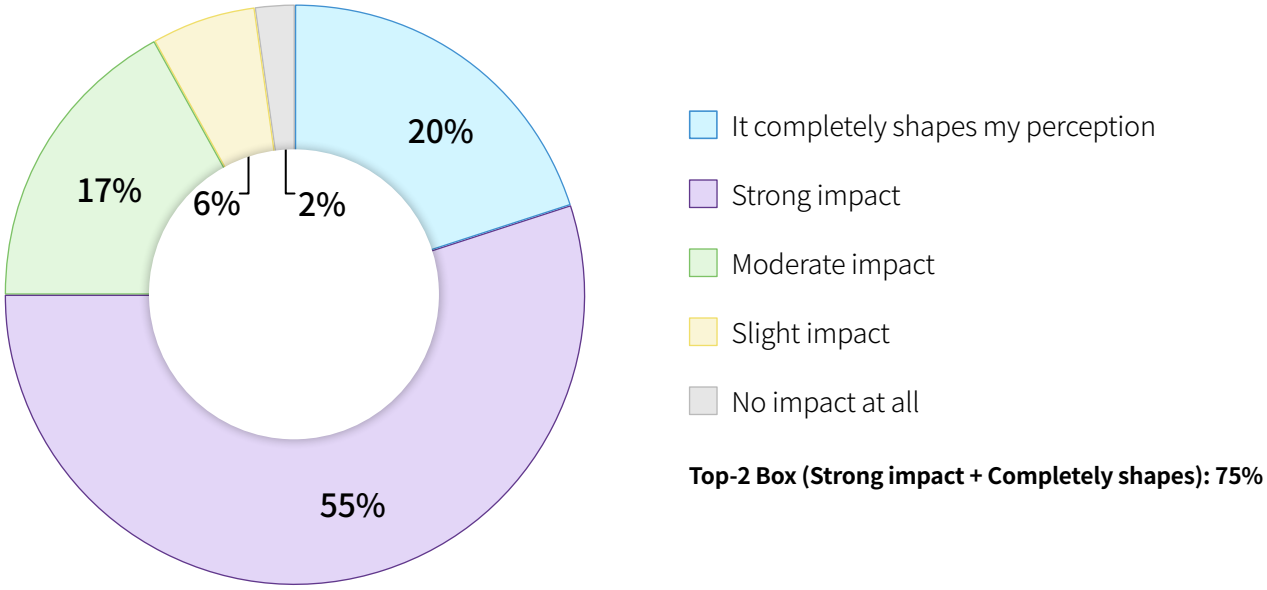
Takeaway for the C-Suite

Consumers don't trade off between a call that connects and a call that sounds clear. They demand both at 81% intensity. CIOs evaluating voice infrastructure must reject the false choice between reliability and quality — and invest in architecture that delivers both simultaneously. Avaya Nexus™ was purpose-built for exactly this standard.

3: Voice Quality as Universal Brand Signal — Even Retail Gets Judged

Question:

How much does the voice quality of a phone call (crystal clear vs. staticky or garbled) affect your perception of a retail business like a restaurant or department store?



Top-2 Box (Strong impact + Completely shapes): 75%

Key Insight

75% of consumers say voice quality strongly shapes their perception of a business — even a restaurant is judged by how its phone sounds. This is not a critical-services phenomenon. It is universal. The phone connection functions as a proxy for operational competence across every industry.

What It Means for Businesses

If the phone sounds bad, the business seems bad — regardless of whether it's a hospital or a hardware store. This finding demolishes the assumption that voice quality only matters in high-stakes verticals. Consumers apply the same judgment to every organization they call.

Voice quality operates as an unconscious competence signal. Consumers may not articulate it in a feedback survey, but they feel it — and they act on it. Three-quarters of them say so explicitly when asked directly. The remaining 25% aren't saying it doesn't matter; most of them (17%) still acknowledge a moderate impact.

- 75% of consumers say voice quality shapes their perception of even a retail business. The standard is universal.
- Voice quality operates below conscious awareness as a proxy for institutional competence.
- Any organization with a phone number is being evaluated on the quality of its voice infrastructure — whether it realizes it or not.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that invest in high-fidelity voice infrastructure create an immediate, unconscious perception of competence and professionalism — before a single word of substance is exchanged.

Risk:

- Poor voice quality doesn't just frustrate callers — it degrades the brand. Consumers who experience staticky or garbled audio carry that perception forward into every subsequent interaction with the organization.

Action:

- Treat voice infrastructure as a brand asset, not a facilities expense.
- Prioritize wideband, high-fidelity audio across all customer-facing voice touchpoints.
- Audit current voice quality against the standard that 75% of consumers are applying — and close any gaps before competitors do.

Final Thought

Voice quality is the invisible handshake. Before a caller hears the agent's words, they've already heard the organization's infrastructure — and they've already started forming a judgment. That judgment is instant, unconscious, and difficult to reverse.

Why You Need Avaya Nexus

Framing the Experience:

This research confirms that voice quality is a universal brand signal — not a vertical-specific concern. The most successful organizations are those that:

- Treat every phone connection as a brand interaction
- Invest in voice infrastructure that signals competence before a word is spoken
- Recognize that the quality of the connection shapes the perception of the entire organization

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees voice quality as the first impression — and the lasting one.
- With Avaya Nexus™, organizations deliver high-fidelity voice that functions as a competence signal, reinforcing trust at the infrastructure level.

How the Data Maps to Experience Shifts

From	To
Voice quality as a technical metric	Voice quality as a brand signal
"Good enough" audio	High-fidelity audio as standard
Perception shaped by marketing	Perception shaped by the phone connection
Voice infrastructure as a back-office cost	Voice infrastructure as front-line brand asset

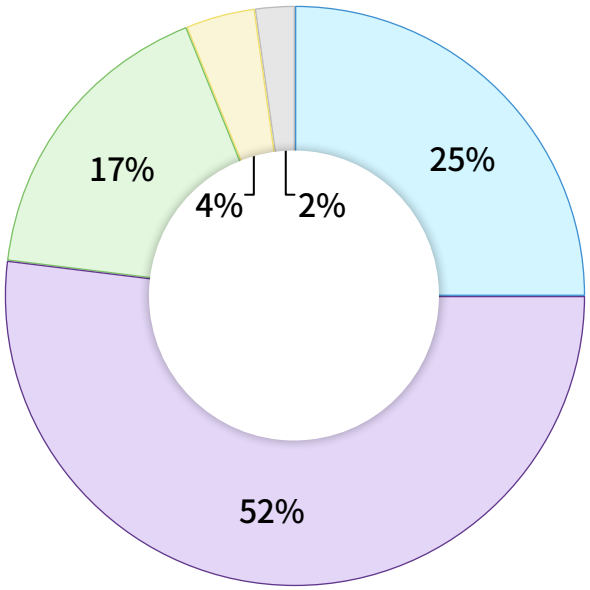
Takeaway for the C-Suite

Voice quality is a universal brand signal. 75% of consumers — across every industry, not just critical services — judge an organization by how its phone sounds. This means voice infrastructure isn't an IT line item. It's a brand investment. Organizations that deliver crystal-clear, high-fidelity voice on every call project competence. Those who don't project the opposite.

4: The Universal Standard — Hospitals and Banks Are Judged on the Same Curve

Question:

How much does the voice quality of a phone call (crystal clear vs. staticky or garbled) affect your perception of a critical services business like a hospital or bank?



Top-2 Box (Strong impact + Absolutely shapes): 77%

Key Insight

76% of Americans say voice quality shapes their perception of hospitals and banks — matching the 75% who say the same about retail. The standard is universal. Consumers do not grade critical-services organizations on a different curve. They hold everyone to the same expectation.

What It Means for Businesses

The real story is the gap that doesn't exist. There is no premium tier of expectation reserved for hospitals and banks. Consumers already hold every business to the highest standard. The narrative shifts from "critical services demand more" to "every business is judged equally — and critical services simply can't afford to fail that test."

For CIOs in healthcare, financial services, and government, this finding reinforces a foundational truth: voice quality isn't just a regulatory requirement. It is a consumer expectation that aligns with the standards they apply to every organization they interact with. The consumer doesn't make a distinction between a bank and a burger joint — and neither should the infrastructure decision.

- The near-identical results between retail (75%) and critical services (77%) reveal a universal standard.
- For critical-services organizations, voice quality is both a consumer expectation and a regulatory imperative — a dual mandate.
- The excuse that "we're not a critical service, so voice quality isn't a priority" is eliminated by this data. Every organization is held to the same standard.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Critical-services organizations can leverage their existing investment in reliability and compliance to meet a consumer expectation they're already positioned to exceed — turning infrastructure into a competitive advantage.

Risk:

- Organizations in regulated industries that treat voice quality as "good enough" are failing to meet a standard that consumers universally apply. The margin for error is zero, because consumers don't grade on a curve.

Action:

- Benchmark voice quality against the universal standard, not against industry-specific minimums.
- Recognize that the consumer's expectation for a hospital call is identical to their expectation for a restaurant call — the stakes are just higher when the infrastructure fails.
- Deploy a purpose-built voice infrastructure that exceeds the universal standard, not merely meets it.

Final Thought

Consumers don't lower their expectations for organizations that serve critical functions. If anything, they raise them — but they start from the same baseline they apply to everyone else. The universal standard means that critical-services organizations must lead on voice quality, not merely match.

Why You Need Avaya Nexus

Framing the Experience:

This data eliminates the last excuse for underinvestment in voice infrastructure. The consumer's voice-quality standard is universal, and critical services organizations face the greatest consequences for failing it. The most successful organizations:

- Meet the universal standard as a baseline
- Exceed it as a differentiator
- Build on purpose-designed infrastructure that makes exceeding the standard a system-level guarantee, not a best-effort aspiration.

Empowering the Critical Communications Mindset:

- A mission-critical mindset doesn't ask whether voice quality matters in its industry. It knows the consumer has already made a decision.
- With Avaya Nexus™, critical-services organizations deliver voice quality that exceeds the universal standard — backed by an architecture designed for exactly the environments where failure carries the highest consequences.

How the Data Maps to Experience Shifts

From	To
Industry-specific voice quality standards	A universal consumer standard across all industries
"We're not a critical service, so it doesn't matter."	Every organization is judged equally
Meeting the regulatory minimum	Exceeding the consumer's expectation
Voice quality as a compliance checkbox	Voice quality as competitive differentiation

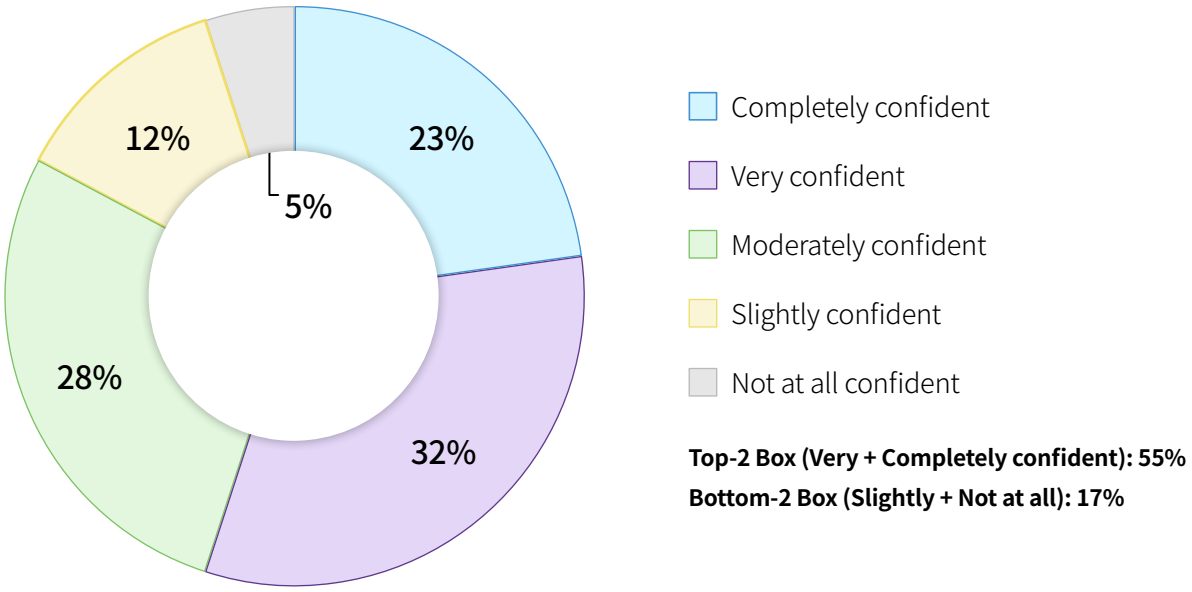
Takeaway for the C-Suite

Consumers hold hospitals and banks to the same voice-quality standard they apply to restaurants and retail. The gap doesn't exist. For critical-services CIOs, this means your regulator doesn't set the bar — your consumer sets it. 77% of them are judging you on every call. Avaya Nexus™ delivers the infrastructure to exceed that standard — not just meet it.

5: The Emergency Confidence Divide — Nearly Half of Americans Have Doubts

Question:

Imagine a severe weather emergency hits your region. How confident are you that your hospital, bank, or utility company could still reach you — or you them — by phone without delay?



Top-2 Box (Very + Completely confident): 55%
Bottom-2 Box (Slightly + Not at all): 17%

Key Insight

Nearly half of Americans lack confidence that their hospital or bank could reach them during a severe emergency. While 55% express high confidence, 45% do not — and nearly 17% have little to no confidence. The infrastructure trust gap is real.

What It Means for Businesses

The story is about the 45% who lack high confidence, not the 55% who have it. The crowded middle — 28% who are only "moderately confident" — is the persuadable segment. In a life-or-death scenario, "moderate confidence" is not confidence at all.

For critical-service providers, the question is simple: can you afford to have nearly half your customers doubting whether you can reach them when it matters most? Every dollar invested in resilient, zero-downtime voice infrastructure closes that gap. Every outage, every degradation, every silent failure widens it.

- 45% of consumers lack high confidence that essential service providers could reach them during a severe emergency.
- The 28% "moderately confident" cohort is the persuadable middle — their confidence is shaped directly by infrastructure investment decisions.
- The infrastructure trust gap is a measurable liability for every critical-services organization, and it widens with every publicized failure.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that can demonstrably prove their resilience during emergencies — through uptime records, redundancy architecture, and real-world performance — convert the persuadable middle into loyal, high-confidence customers.

Risk:

- A single publicized failure during an emergency doesn't just damage the organization that failed — it erodes confidence across the entire sector. The trust gap is contagious.

Action:

- Architect for worst-case scenarios, not average conditions. Dual-Availability Zone deployment ensures continuous operations even during partial failures or complete AZ outages.
- Invest in real-time health monitoring and proactive failover — don't wait for the emergency to discover the vulnerability.
- Communicate resilience investments to customers and stakeholders. The trust gap exists partly because consumers don't know what's protecting them.

Final Thought

The infrastructure trust gap isn't abstract. It's 45% of the public carrying a quiet doubt about whether the organizations they depend on can reach them when the weather turns, the grid fails, or the emergency hits. Closing that gap is an infrastructure decision—and only purpose-built infrastructure for zero downtime can close it.

Why You Need Avaya Nexus

Framing the Experience:

This data reveals a public that wants to trust its critical-service providers but isn't sure it can. The organizations that close the trust gap are those that:

- Architect for zero downtime — not as an aspiration, but as a design principle
- Deploy a Dual-Availability Zone infrastructure that maintains operations through partial and complete failures
- Treat resilience as a brand promise, not a technical specification

Empowering the Critical Communications Mindset:

- A mission-critical mindset doesn't accept "moderately confident" as good enough. It engineers for "completely confident."
- With Avaya Nexus™, organizations deploy the infrastructure that turns the 45% trust gap into a trust asset — because when the emergency hits, the platform doesn't fail.

How the Data Maps to Experience Shifts

From	To
Hoping the system holds during an emergency	Engineering the system to guarantee it
Accepting "moderate confidence" as sufficient	Targeting "complete confidence" as the standard
Reacting to outages after the fact	Proactive failover and health monitoring
Resilience as a technical specification	Resilience as a public trust obligation

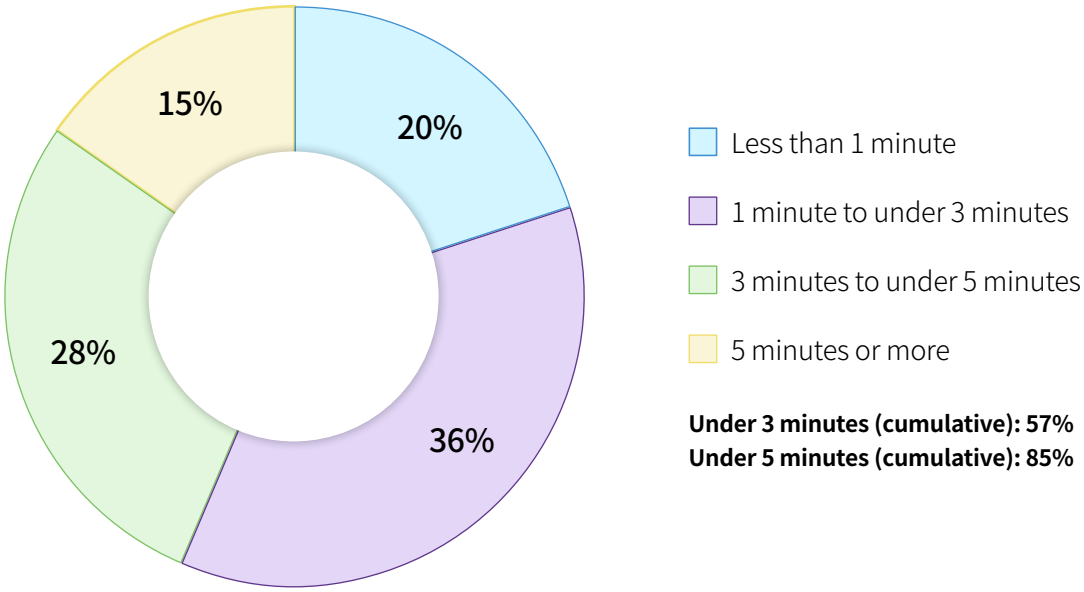
Takeaway for the C-Suite

45% of consumers doubt that their hospital, bank, or utility can reach them during a severe emergency. That's not a technology statistic — it's a public trust deficit. CIOs who invest in zero-downtime, Dual-AZ voice infrastructure don't just upgrade their systems — they close the trust gap. Avaya Nexus™ was engineered for exactly this: the moments when confidence in the infrastructure is the difference between public trust and public doubt.

6: The 3-Minute Cliff — How Fast Consumers Lose Faith

Question:

You are calling your bank or hospital to report an urgent, time-sensitive crisis. How long does a "silent hold" — where a transfer rings continuously or goes dead silent — have to last before you lose faith that the organization is competent?



Under 3 minutes (cumulative): 57%
Under 5 minutes (cumulative): 85%

Key Insight

The 3-Minute Cliff: 57% of consumers lose faith in their bank or hospital before the silent hold hits 3 minutes — and 85% are gone before 5. One in five loses faith in under sixty seconds. This isn't a patience problem. It's a competence judgment rendered in real time.

What It Means for Businesses

Silent hold during a crisis is interpreted as institutional failure, and the window for recovery is measured in seconds, not minutes. The cumulative framing tells the story: at 57% under three minutes and 85% under five, there is a cliff — not a gradual decline — in consumer confidence.

The 1-in-5 who break in under a minute are the emotional headline. These consumers aren't impatient — they're terrified. They've called because something is wrong, and the silence on the other end confirms their worst fear: nobody is in control.

- 57% lose faith in under 3 minutes. 85% are gone before 5. The window is measured in seconds, not minutes.
- A silent hold isn't seen as a technical delay — it's seen as institutional incompetence.
- One in five consumers loses faith in under 60 seconds. For a caller in crisis, silence is the loudest signal of all.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that eliminate silent hold scenarios — through intelligent routing, seamless failover, and proactive caller engagement — turn a universal pain point into a moment of differentiation.

Risk:

- Every second of silent hold during a crisis call compounds the competence judgment. The damage isn't linear — it's exponential. Consumers don't gradually lose faith; they fall off a cliff.

Action:

- Deploy carrier-grade SIP routing with intelligent call distribution to eliminate silent hold at the infrastructure level.
- Engineer seamless failover across availability zones so that transfers never result in dead air or endless ringing.
- Monitor and measure silent-hold duration as a critical KPI — not a secondary metric buried in call-center reporting.

Final Thought

The 3-minute cliff is not a call-center problem. It is an infrastructure problem. No amount of agent training, scripting, or workforce optimization can compensate for an architecture that leaves callers in silence when they need reassurance most. The fix is in the platform, not the playbook.

Why You Need Avaya Nexus

Framing the Experience:

This data quantifies what every caller already feels: silence during a crisis is the death of trust. The organizations that avoid the 3-minute cliff are those that:

- Engineer call routing and transfer at the infrastructure level — not as a software overlay on a best-effort platform
- Deploy next-generation session services with carrier-grade SIP routing for seamless, silent-hold-free transfers
- Treat every second of silence as a measured trust liability

Empowering the Critical Communications Mindset:

- A mission-critical mindset measures trust in seconds, not minutes.
- With Avaya Nexus™, the next-generation session services and Dual-AZ architecture ensure that calls are connected, routed, and transferred without the silent-hold failures that destroy consumer confidence — because in critical environments, silence isn't golden. It's catastrophic.

How the Data Maps to Experience Shifts

From	To
Measuring hold time as an average	Measuring the silent hold as a cliff
Treating transfers as a call-center workflow	Engineering transfers as an infrastructure function
Accepting some silent hold as inevitable	Targeting zero silent hold as the standard
Patience is the consumer's responsibility	Competence is the institution's obligation

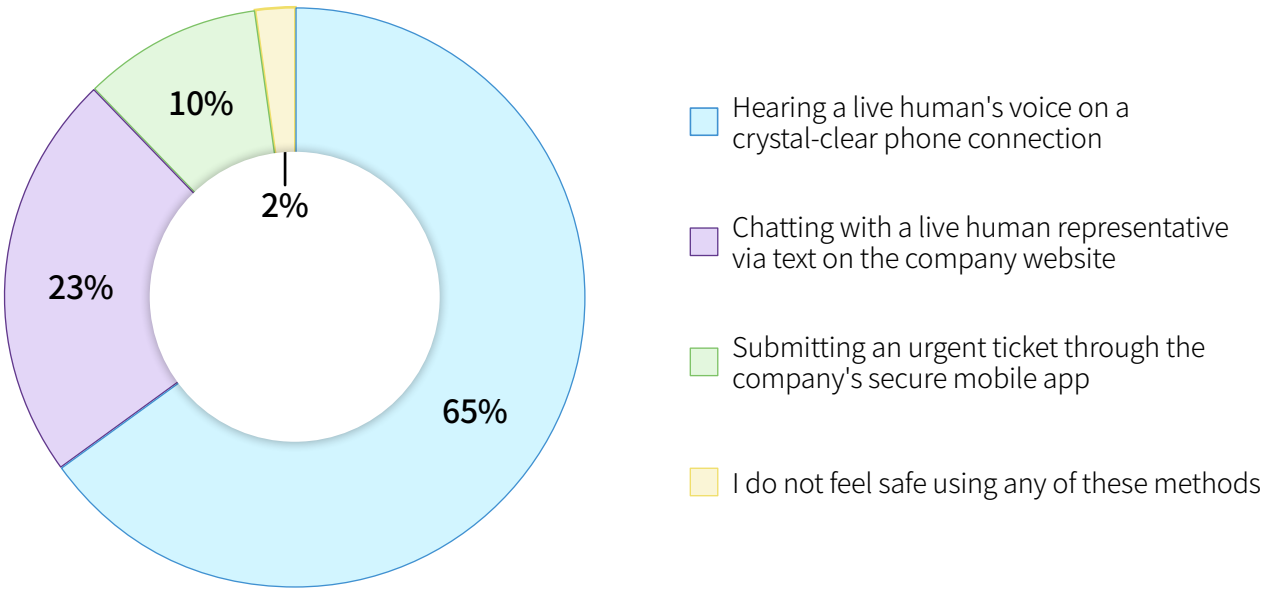
Takeaway for the C-Suite

85% of consumers lose faith before a silent hold reaches 5 minutes. 57% are gone before 3. This is not a workforce problem — it is an infrastructure problem. CIOs must invest in carrier-grade routing and seamless failover to eliminate silent holds at the architectural level. Avaya Nexus™ delivers exactly this: next-generation session services engineered so that the silence never happens.

7: The Voice-First Security Hierarchy — 65% Say Only a Human Voice Delivers Safety

Question:

Imagine you discover a massive, unauthorized transfer out of your bank account, or you are waiting on a critical medical test result. Which of the following communication methods makes you feel the most secure and safe that your issue is actually being handled?



Key Insight

65% of Americans say only a crystal-clear human voice makes them feel secure during a financial or medical crisis. Digital channels cannot replace the phone. Chat captures 23%, app-based tickets just 10%. And only 2% say nothing would make them feel safe — meaning 98% believe a solution exists, and the overwhelming majority say that solution is voice.

What This Reveals

This is not generational nostalgia. It is a neurological reality: the human voice carries trust signals — tone, pacing, emotional resonance — that text cannot replicate. When consumers face a financial crisis or a medical scare, they don't want a chatbot, a ticket number, or a text thread. They want to hear a human voice, and they want that voice to be crystal clear.

The 65% finding is the single strongest proof point for the voice infrastructure thesis. It tells every CIO evaluating channel strategy that voice is not a legacy channel being replaced by digital — it is the primary trust channel that digital cannot replicate.

- 65% choose voice as the only channel that delivers genuine security during a crisis. This is a mandate, not a preference.
- 98% believe a solution exists for feeling safe — and the dominant answer is voice.
- The quality of the voice connection is inseparable from the trust it delivers. A garbled voice call undermines the very safety signal consumers are seeking.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that invest in crystal-clear, always-available voice infrastructure position themselves as the trusted channel of last resort — the one consumers reach for when the stakes are highest.

Risk:

- Organizations that deprioritize voice in favor of digital-first or chatbot-first strategies risk removing the one channel that 65% of consumers say delivers genuine security during a crisis.

Action:

- Ensure voice remains the primary, always-available channel for high-stakes interactions — not a fallback behind digital deflection strategies.
- Invest in high-fidelity audio infrastructure that preserves the paraverbal signals — tone, cadence, breath — that transmit trust.
- Design channel strategy around the consumer's trust hierarchy, not the organization's cost hierarchy.

Final Thought

The human voice is not a legacy channel. It is the trust channel. When everything else fails — when the app crashes, the chatbot loops, the email goes unanswered — consumers reach for the phone because they know that hearing a human voice on a clear connection is the fastest path to feeling safe. The infrastructure behind that voice is what makes the trust real.

Why You Need Avaya Nexus

Framing the Experience:

This data confirms what neuroscience already tells us: the human voice is the most powerful trust signal available. The organizations that harness this finding are those that:

- Prioritize voice as the primary trust channel — not a cost-center to be deflected
- Invest in high-fidelity voice infrastructure that preserves the emotional nuance consumers depend on
- Build their channel strategy around consumer psychology, not operational convenience

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees voice not as a channel to be optimized away, but as the foundation of consumer trust.
- With Avaya Nexus™, organizations deliver the crystal-clear, high-fidelity voice that 65% of consumers say is the only thing that makes them feel safe — backed by zero-downtime infrastructure that keeps the voice available when it's needed most.

How the Data Maps to Experience Shifts

From	To
Digital-first channel strategy	Trust-first channel strategy
Voice as a legacy channel to be retired	Voice as the primary trust channel
Optimizing for cost-per-interaction	Optimizing for trust-per-interaction
Chatbots as the default escalation path	Human voice as the default for high-stakes moments

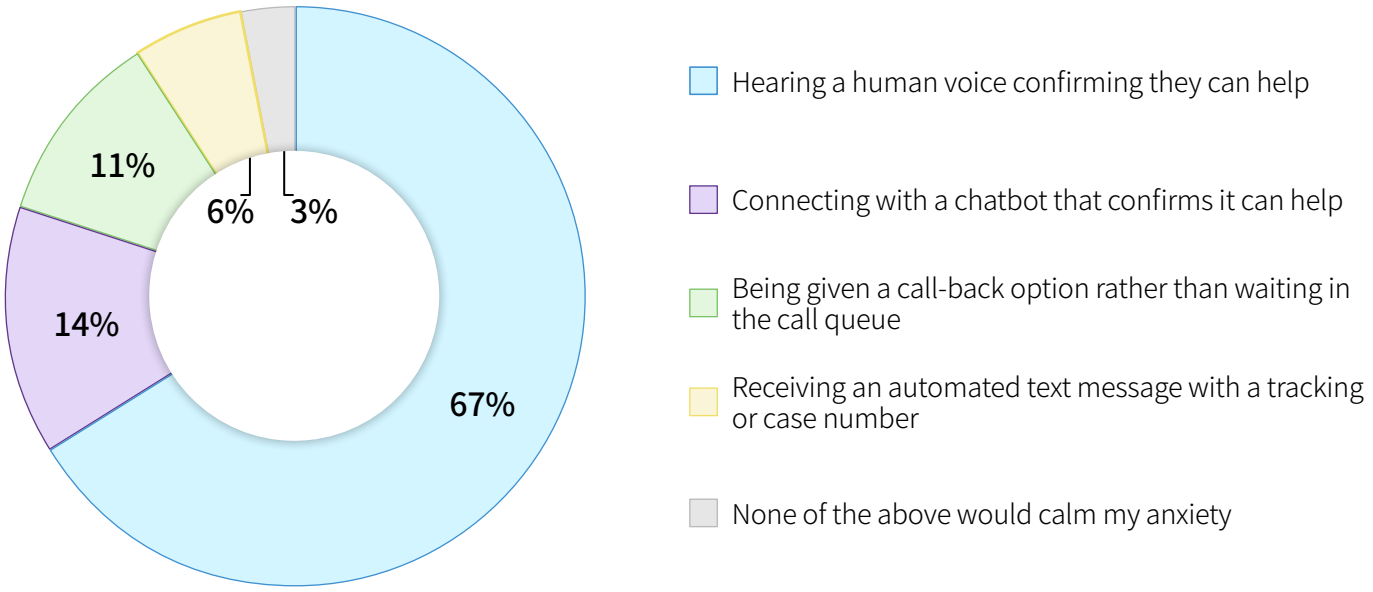
Takeaway for the C-Suite

65% of consumers say only a crystal-clear human voice delivers genuine security during a crisis. This isn't a channel preference — it's a trust architecture. CIOs who invest in high-fidelity, always-on voice infrastructure aren't preserving a legacy channel. They're investing in the one channel that delivers what digital cannot: the physiological experience of safety. Avaya Nexus™ is purpose-built to deliver that experience — with the reliability, clarity, and resilience that trust demands.

8: The Anxiety Circuit Breaker — A Human Voice Outscores Chatbots 5 to 1

Question:

You are in a state of panic over a canceled flight, a lost credit card, or an urgent medication refill. You reach out to the company for help. What has the greatest immediate impact on lowering your heart rate and calming your anxiety?



Key Insight

67% of panicking consumers say only a human voice calms them down — chatbots score under 14%. The human voice outscores chatbots nearly 5 to 1 and automated texts more than 12 to 1 as an anxiety circuit breaker. This is not about information delivery. It is about emotional regulation.

What This Reveals

The 67% finding is even stronger than the 65% voice-first security result in Q7, suggesting that the physiological calming effect of voice may be more powerful than its informational security effect. This is biology, not sentiment. The human voice transmits paraverbal signals — tone, cadence, breath, emotional warmth — that activate calming responses in the listener's nervous system. No chatbot, no matter how sophisticated, can replicate this.

Organizations that route panicking customers to chatbots aren't saving money — they're prolonging crisis states and compounding the emotional damage. The cost of a chatbot interaction that fails to calm a panicking consumer isn't measured in handle time. It's measured in terms of trust destruction, negative word of mouth, and customer attrition.

- 67% say a human voice is the greatest immediate calming mechanism during a panic state. The ratio vs. chatbots is 5 to 1.
- Voice delivers a physiological calming effect that digital channels cannot replicate — this is neuroscience, not nostalgia.
- Routing panicking customers to chatbots doesn't reduce cost — it compounds the crisis and accelerates trust destruction.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that ensure a human voice is available on a crystal-clear connection instantly during crisis moments become the brands that calm, reassure, and retain — while competitors resort to chatbots and lose.

Risk:

- Every chatbot interaction with a panicking consumer that fails to resolve the emotional state — not just the transactional query — is a compounding trust liability.

Action:

- Design escalation paths that prioritize speed-to-human-voice during crisis interactions — not speed-to-chatbot.
- Ensure the voice connection is crystal clear. A garbled, clipped human voice doesn't calm anxiety — it amplifies it.
- Measure the emotional outcome of interactions, not just the transactional resolution. A resolved ticket and a calmed consumer are not the same thing.

Final Thought

The human voice is the original anxiety circuit breaker. It predates every digital channel, every chatbot, every automated text — and it still outperforms them all by a factor of five. The infrastructure question isn't whether to invest in AI or voice. It's whether the voice infrastructure is good enough to deliver the calming signal that 67% of consumers are counting on.

Why You Need Avaya Nexus

Framing the Experience:

This data reveals that voice infrastructure is not just a communications tool — it is a crisis management tool. The organizations that use it effectively are those that:

- Ensure instant access to a human voice on a crystal-clear connection during crisis moments.
- Invest in high-fidelity audio that preserves the emotional nuance — the sighs, the reassurance, the calm — that calms a panicking consumer.
- Treat the voice connection as the first line of emotional defense, not the last resort after digital channels fail

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees the voice connection as an anxiety circuit-breaker—not a cost to be minimized.
- With Avaya Nexus™, the infrastructure ensures that when a panicking consumer reaches for the phone, the connection is crystal clear, the failover is seamless, and the platform beneath it never compromises the voice on the other end.

How the Data Maps to Experience Shifts

From	To
Chatbot-first escalation paths	Human-voice-first for crisis moments
Measuring handle time	Measuring emotional resolution
Voice as a costly fallback	Voice as the primary crisis management channel
Optimizing for deflection	Optimizing for calming

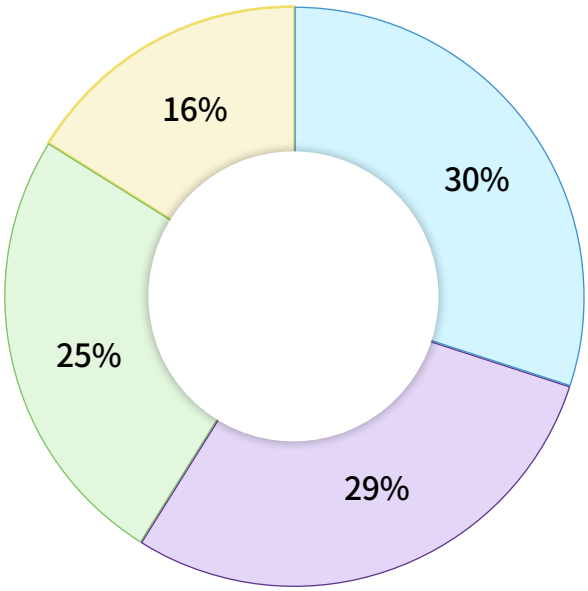
Takeaway for the C-Suite

67% of panicking consumers say only a human voice calms them down. Chatbots score 14%. This isn't a customer preference survey — it's a neuroscience finding with direct business implications. Organizations that invest in crystal-clear, always-on voice infrastructure aren't just resolving tickets; they're also improving customer experience. They're calming crises. Avaya Nexus™ delivers the high-fidelity, zero-downtime voice platform that makes the human voice available — and effective — precisely when consumers need it most.

9: The Fraud Spiral — One Dropped Call Creates a Full-Blown Crisis

Question:

You receive an urgent, automated text from your bank stating, "Suspicious Activity Detected: Call Us Immediately."
You dial the number, but the phone rings endlessly and then drops. What is your immediate, gut-level assumption?



- My money is actively being stolen right now, and the bank has lost control
- The text message was probably a scam
- The bank is just experiencing a temporary phone outage, but my money is likely safe
- My account is probably locked down as a precaution, so I will just wait patiently

Catastrophic assumption (stolen + scam combined): 59%

Key Insight

59% of consumers assume the worst when a dropped call follows a bank fraud alert. 30% believe their money is actively being stolen. 29% assume the alert itself was a scam — meaning the bank loses credibility either way. Only 16% respond with patience. The consumer does not give institutions the benefit of the doubt when communication fails during a crisis.

What This Reveals

This is the fraud spiral: a single communication failure transforms a manageable fraud alert into a full-blown crisis of confidence. The bank doesn't just lose the call — it loses control of the narrative. The consumer is left with two equally damaging conclusions: either my money is being stolen, or the bank is so unreliable that I can't tell the difference between a real alert and a phishing attempt.

Only 25% give the bank the benefit of the doubt as a temporary outage. The overwhelming majority do not. The standard is absolute: if you send me an alert, you must be reachable when I call. The fraud alert without a functioning phone system doesn't protect the customer — it terrorizes them.

- 59% make a catastrophic assumption when a dropped call follows a fraud alert. The bank loses either way.
- Only 16% respond with patience. Consumers do not give institutions the benefit of the doubt during a communication failure.
- The fraud spiral transforms a routine security process into a reputational catastrophe — and the trigger is a single dropped call.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that pair their security alert systems with guaranteed-available voice infrastructure turn fraud alerts into trust-building moments — demonstrating competence precisely when consumers are most vigilant.

Risk:

- Any disconnection between outbound alerts and inbound availability creates a fraud spiral: the alert designed to protect the customer becomes the trigger for panic, confusion, and reputational damage.

Action:

- Ensure that a zero-downtime inbound voice system backs every outbound alert channel (text, email, push notification). The alert and the phone must be architecturally linked.
- Deploy infrastructure with guaranteed failover so the phone system remains reachable at the exact moment the alert appears on the consumer's screen.
- Stress-test the full alert-to-call chain under load — not just the alert system or the phone system in isolation.

Final Thought

The fraud spiral reveals a truth that goes beyond financial services: the communication system is the crisis management system. When the two are separated — when an alert goes out, but the phone goes down — the institution doesn't just fail technically. It fails psychologically. The consumer's trust doesn't erode gradually. It collapses in the time it takes for a call to drop.

Why You Need Avaya Nexus

Framing the Experience:

This data reveals that voice infrastructure is inseparable from security infrastructure. The organizations that prevent the fraud spiral are those that:

- Architect voice systems for zero downtime — so the phone is always reachable when the alert hits
- Deploya Dual-Availability Zone infrastructure that maintains call reception even during partial failures or complete AZ outages.
- Treat the inbound call as the final, most critical link in the security chain — not an afterthought.

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees the phone system as the last line of defense in a security event — not a separate system managed by a separate team.
- With Avaya Nexus™, the zero-downtime architecture ensures that when a fraud alert is issued, the phone system captures every call — because in financial services, a dropped call after a fraud alert isn't a technical failure. It's an institutional one.

How the Data Maps to Experience Shifts

From	To
Security alerts and phone systems are separate functions	Security alerts and voice infrastructure as a single chain
Accepting occasional phone system downtime	Zero-downtime voice as a security requirement
Fraud alerts as customer protection	Fraud alerts without voice backup as customer terrorism
Hoping the phone system is available	Guaranteeing the phone system is available

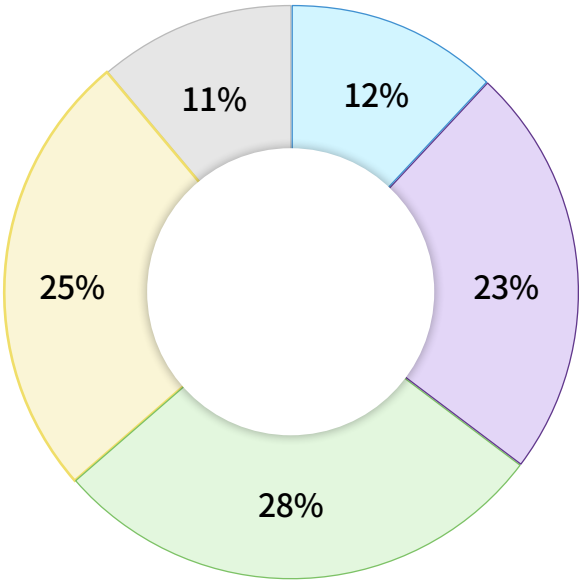
Takeaway for the C-Suite

59% of consumers make a catastrophic assumption when a dropped call follows a fraud alert. Only 16% respond with patience. For financial services CIOs, this means the phone system isn't just IT infrastructure — it is the final link in the security chain. If the alert fires but the phone fails, the institution has created the very crisis it was trying to prevent. Avaya Nexus™ delivers a zero-downtime, Dual-AZ voice infrastructure that ensures the phone is always there when the alert hits — because in financial services, a dropped call after a fraud alert isn't a technical failure. It is an institutional crisis.

10: The Trust Erosion Curve — 89% Say a Single Failure Costs Trust

Question:

If you were to experience a communication failure with an essential service provider — for example, a dropped call with your bank or garbled audio with your doctor's office — how does it affect your trust in that organization?



Any trust reduction (Slightly through Completely): 89%
Significant damage (Noticeably + Seriously + Completely): 64%

Key Insight

89% of consumers say a single communication failure erodes their trust in an essential service provider. Only 11% say it has no lasting effect. For nearly two-thirds (64%), the damage crosses the threshold from "slight" to "noticeable," "serious," or "destruction." Every dropped call, every garbled connection, every silent hold is a trust event with measurable consequences.

What This Reveals

The near-universality of trust erosion is the headline. Nine in ten consumers are keeping score. A single dropped call with a bank, a single garbled connection with a doctor's office, a single silent hold with a utility company — each one registers as a trust event in the consumer's mental ledger.

The 64% who experience significant damage are the most consequential cohort. These aren't consumers who shrug and move on. They're consumers who update their internal model of the organization downward. The 12% who say their trust is destroyed represent the most extreme response: a single interaction failure that severs the relationship entirely.

Communication infrastructure is not a cost center. It is a trust asset — and 89% of consumers are keeping score.

- 89% of consumers say a single communication failure erodes their trust. Only 11% are unaffected.
- For 64%, the damage is noticeable or worse — crossing the threshold from minor irritation to a meaningful reduction in trust.
- 12% say a single failure destroys their trust. For these consumers, there is no second chance.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that achieve consistent, failure-free communication don't just avoid trust erosion—they accumulate trust capital. Every successful interaction reinforces the perception that the institution is competent, reliable, and in control.

Risk:

- The trust erosion curve is asymmetric: a single failure costs more trust than a single success earns. Organizations operating on infrastructure prone to intermittent failures are bleeding trust faster than they can rebuild it.

Action:

- Treat every communication interaction as a trust event with measurable consequences — not as a routine operational transaction.
- Invest in infrastructure that eliminates intermittent failures, not just catastrophic outages. The consumer doesn't distinguish between a five-second audio dropout and a full system crash — both register as trust events.
- Measure communication reliability as a trust metric, not just an uptime metric. 99.9% uptime still allows enough failures to erode trust across a large customer base.

Final Thought

Trust isn't built through marketing campaigns. It is built — or destroyed — in the moments when a consumer reaches for the phone and either connects clearly or doesn't. The 89% finding indicates that virtually every consumer is evaluating the institution's competence based on their communication experience. The infrastructure behind that experience is the most consequential trust investment an organization can make.

Why You Need Avaya Nexus

Framing the Experience:

This data reframes communication infrastructure as the organization's largest trust asset — or its largest trust liability. The organizations that accumulate trust capital are those that:

- Engineer for zero communication failures — not just zero catastrophic outages
- Recognize that every interaction is a trust event evaluated by 89% of consumers
- Deploy infrastructure where reliability is deterministic, not probabilistic

Empowering the Critical Communications Mindset:

- A mission-critical mindset treats every call as a trust transaction. The balance goes up or down — never stays flat.
- With Avaya Nexus™, organizations deploy a zero-downtime architecture that protects the trust asset on every interaction — because the platform was engineered to eliminate the failures that 89% of consumers say they will never forget.

How the Data Maps to Experience Shifts

From	To
Communication failures as operational incidents	Communication failures as trust events
Measuring uptime as a technical metric	Measuring reliability as a trust metric
Trust built through marketing and brand	Trust built — or destroyed — on every call
Infrastructure as a cost center	Infrastructure is the organization's largest trust asset

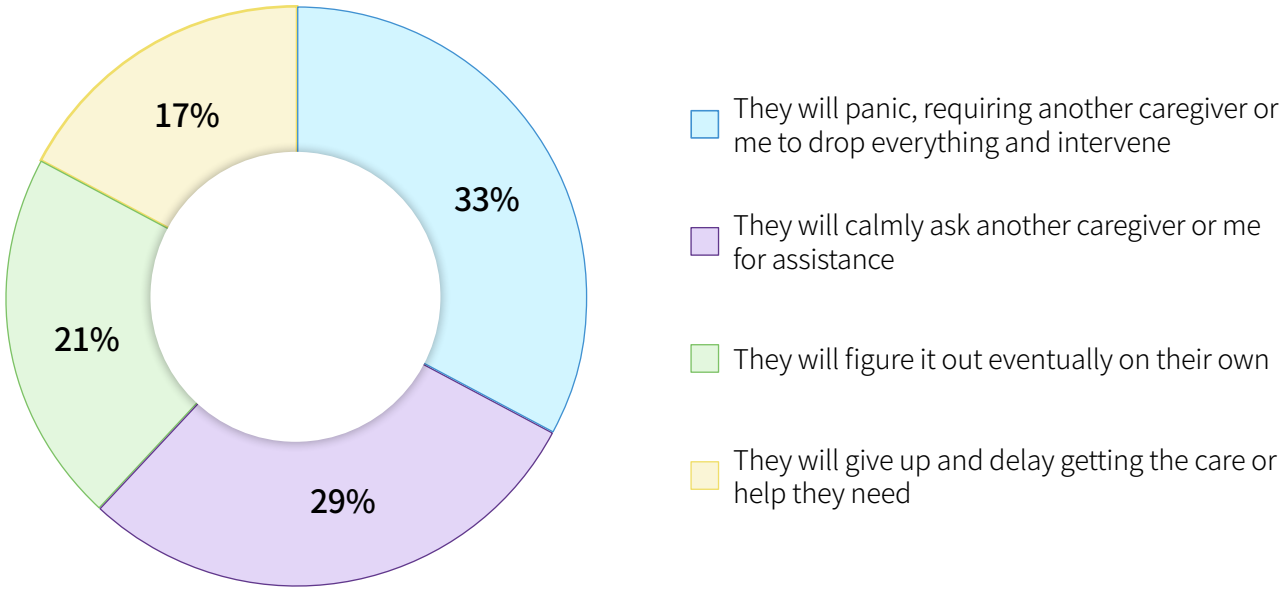
Takeaway for the C-Suite

89% of consumers say a single communication failure erodes their trust. 64% say the damage is significant. 12% say it's total. This is not an IT metric — it is a trust metric with direct implications for retention, loyalty, and lifetime value. Every communication failure is a trust withdrawal that the organization must work to recover — and some withdrawals are fatal. Avaya Nexus™ delivers the zero-downtime, carrier-grade reliability that keeps the trust account in surplus — because in mission-critical environments, the infrastructure is the trust.

11: The Vulnerability Multiplier — Communication Failures Have Human Casualties

Question:

Think about an elderly family member, or someone with a disability, trying to navigate a medical or financial emergency over the phone. If the phone system is staticky, requires them to repeat themselves multiple times, or drops the call, what is the most likely outcome?



Key Insight

Half of Americans say poor phone systems will cause vulnerable family members to either panic (33%) or give up entirely on getting care (17%). The "panic" response is the single largest category, meaning consumers believe the most likely outcome of a poor phone connection for a vulnerable person is an escalation that disrupts not just the patient, but the entire family support structure.

What This Reveals

This finding moves the conversation from consumer inconvenience to human consequence. When the phone system fails a vulnerable person — an elderly parent navigating a medical crisis, a person with a disability trying to report a financial emergency — the failure doesn't stay contained. It radiates outward.

The 33% who predict panic aren't describing a mild concern. They're describing a scenario where a caregiver must drop everything — leave work, interrupt their own obligations, absorb the emotional toll — to intervene because the phone system couldn't do its job. The 17% who predict giving up entirely are describing delayed care, untreated conditions, and unresolved financial crises.

Combined, 50% of consumers believe that poor phone infrastructure will cause measurable harm to the most vulnerable people in their lives.

- 50% predict a negative outcome for vulnerable family members: panic (33%) or giving up on care entirely (17%).
- The "panic" response is the plurality — the single most common predicted outcome — meaning poor infrastructure creates cascading disruption across families.
- Only 21% believe a vulnerable person could figure it out on their own. The remaining 79% predict some form of dependency or failure.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that deliver clear, reliable, and accessible voice experiences for vulnerable populations don't just serve those individuals — they earn the loyalty of every caregiver, family member, and advocate connected to them.

Risk:

- Communication failures that affect vulnerable populations carry amplified consequences: cascading caregiver disruption, delayed care, regulatory exposure, and reputational damage that extends far beyond the individual caller.

Action:

- Design voice infrastructure with accessibility and clarity as first-order requirements — not afterthoughts bolted onto a system designed for non-disabled, tech-savvy callers.
- Ensure high-fidelity audio that minimizes repetition. For a vulnerable caller, being asked to repeat themselves isn't a minor inconvenience — it's a barrier to care.
- Test infrastructure under stress conditions that simulate the real-world experience of a vulnerable caller during a crisis — not just average-case scenarios.

Final Thought

Communication infrastructure is not just a technology decision. It is an accessibility decision, a caregiving decision, and — for vulnerable populations — a health and safety decision. The 50% negative-outcome finding tells us that half the public believes current phone systems will fail the people who need them most. That belief is not abstract. It is rooted in lived experience — and it carries consequences that extend far beyond the call.

Why You Need Avaya Nexus

Framing the Experience:

This data reveals that communication infrastructure has human casualties — not metaphorical ones. The organizations that prevent harm to vulnerable populations are those that:

- Engineer voice systems for clarity, reliability, and accessibility as co-equal priorities
- Deliver high-fidelity audio that preserves every word, reducing the need for repetition that exhausts and confuses vulnerable callers.
- Design for the hardest use case — a frightened, elderly caller during a medical emergency — not the average case

Empowering the Critical Communications Mindset:

- A mission-critical mindset measures infrastructure quality not just by uptime statistics, but by the experience of the most vulnerable caller on the most difficult day.
- With Avaya Nexus™, organizations deliver the carrier-grade voice clarity and zero-downtime reliability that vulnerable populations depend on — because when the phone system fails a vulnerable person, the failure isn't technical. It's human.

How the Data Maps to Experience Shifts

From	To
Communication failures as inconveniences	Communication failures as human casualties
Designing for the average caller	Designing for the most vulnerable caller
Measuring impact on the individual	Measuring cascading impact on families and caregivers
Accessibility as a compliance checkbox	Accessibility as a first-order infrastructure requirement

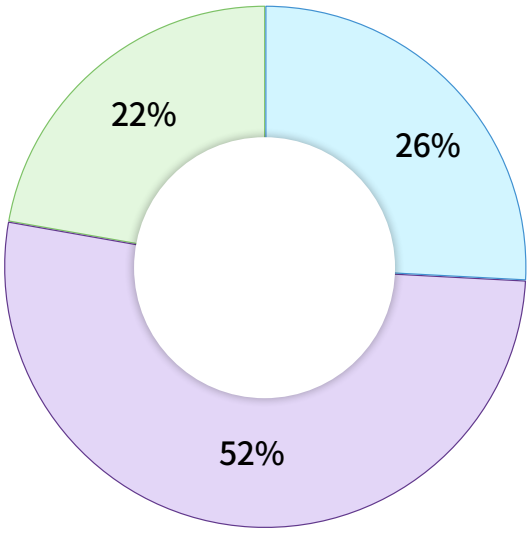
Takeaway for the C-Suite

50% of consumers predict that poor phone systems will cause vulnerable family members to panic or give up on getting care. This is not a customer satisfaction issue — it is a human safety issue with direct implications for regulatory compliance, legal liability, and brand reputation. For healthcare, financial services, and government organizations, the voice infrastructure serving vulnerable populations must be purpose-built for clarity, reliability, and accessibility. Avaya Nexus™ delivers that standard — because the consequences of falling short aren't measured in NPS scores. They're measured in delayed care, caregiver disruption, and preventable harm.

12: The Competence Inference — The Connection IS the Competence

Question:

You are in the middle of a frightening emergency and finally reach a professional (like a dispatcher, nurse, or fraud specialist) who is supposed to take charge of the situation. However, their voice keeps clipping in and out due to a poor connection. How does this affect your view of them?



- It has no effect; I still trust they are fully capable
- I have less confidence in the organization's ability to control the situation
- I completely lost confidence in the organization's ability to control the situation

Any loss of confidence (less + completely): 74%

Key Insight

74% of consumers lose confidence in emergency professionals when audio clips are used — even though the professional's competence has nothing to do with the phone system. More than one in five completely lose confidence. The connection IS the competence signal. Poor audio makes competent professionals seem incompetent, and the institution pays the price.

What This Reveals

This is the competence inference: consumers transfer their judgment of the audio connection onto the professional on the other end of the line. A nurse whose voice clips in and out is perceived as less capable — not because her skills have changed, but because the infrastructure beneath her has failed.

The 52% who have "less confidence" are making a rational inference from the information available to them. If the organization can't even maintain a clear phone connection during an emergency, what else can't it manage? The 22% who completely lose confidence represent the most extreme manifestation: a total collapse of institutional trust triggered not by the professional's words or actions, but by the quality of the signal carrying them.

The professional is being judged for the CIO's infrastructure decision. That is the most powerful boardroom argument this data produces.

- 74% lose confidence in the professional when listening to audio clips are used. The connection is the competence signal.
- 22% completely lose confidence — a total trust collapse triggered by infrastructure, not by the professional.
- Competent professionals are made to seem incompetent by the phone system they were given. The CIO's infrastructure decision is the professional's credibility.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that invest in crystal-clear voice infrastructure amplify the perceived competence of every professional on the line — turning infrastructure into a credibility multiplier for the entire workforce.

Risk:

- Poor audio infrastructure doesn't just frustrate callers; it also undermines the quality of service. It actively undermines the perceived competence of skilled professionals — nurses, dispatchers, fraud specialists — creating reputational damage that compounds with every degraded call.

Action:

- Recognize that voice infrastructure is a tool for workforce credibility. The clarity of the connection directly affects the professional's perceived competence.
- Invest in high-fidelity, wideband audio that preserves every word, every nuance, and every reassuring tone — especially in high-stakes interactions where consumer anxiety is already elevated.
- Quantify the cost of the competence inference: how many professional-consumer interactions are degraded by infrastructure that the professional didn't choose and can't control?

Final Thought

The cruelest irony in the data: the professionals who are best trained to handle emergencies — dispatchers, nurses, fraud specialists — are the ones most frequently undermined by the infrastructure beneath them. They can't control the phone system. But 74% of consumers judge them as if they can. The only way to protect the professional's credibility is to fix the infrastructure.

Why You Need Avaya Nexus

Framing the Experience:

This data reveals that voice infrastructure is a credibility multiplier — or a credibility destroyer. The organizations that protect their professionals are those that:

- Invest in carrier-grade voice infrastructure that delivers crystal-clear audio on every call
- Recognize that the professional's perceived competence is a direct function of the connection quality
- Treat voice infrastructure as a workforce empowerment tool, not just a communications utility

Empowering the Critical Communications Mindset:

- A mission-critical mindset protects its people by investing in the infrastructure beneath them.
- With Avaya Nexus™, organizations ensure that their most skilled professionals — the nurses, dispatchers, and specialists who handle the hardest moments — are never undermined by the platform they were given. High-fidelity voice on a zero-downtime architecture means the connection amplifies competence instead of destroying it.

How the Data Maps to Experience Shifts

From	To
Judging the professional by their words	Judging the professional by the connection
Infrastructure is invisible to the consumer	Infrastructure as the primary competence signal
Investing in professional training alone	Investing in professional training AND the infrastructure that carries it
CIO decisions are isolated from workforce credibility	CIO infrastructure decisions as workforce credibility decisions

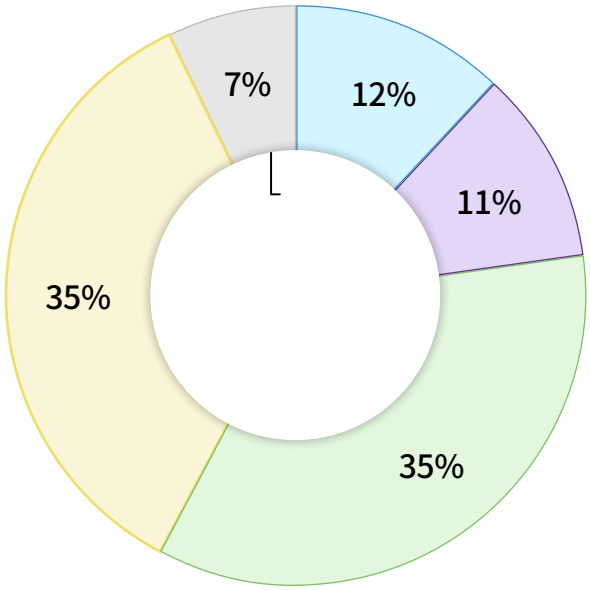
Takeaway for the C-Suite

74% of consumers lose confidence in emergency professionals when audio clips, and 22% lose confidence completely. The professional didn't choose the phone system. The CIO did. Every infrastructure decision that tolerates degraded audio is a decision to undermine the credibility of the organization's most skilled people. Avaya Nexus™ delivers the high-fidelity, carrier-grade voice infrastructure that turns every connection into a competence signal — protecting the professionals who protect the public.

13: The Negative Word-of-Mouth Engine — 93% Will Tell Someone

Question:

After a stressful communication experience with your bank, hospital, or insurance provider, such as dropped calls, long holds, or garbled audio, how likely are you to share that experience with family, friends, or colleagues?



- I would both warn people personally AND post about it publicly
- I would post about it publicly on social media or a review site
- I would actively tell people about it as a warning
- I would mention it casually if it came up in conversation
- I would not mention it to anyone

Active sharing (warn + post + both): 58%

Any sharing (all except "not mention"): 93%

Key Insight

93% of consumers will tell someone after a stressful communication failure with a bank, hospital, or insurer. Only 7% would stay silent. 58% will go beyond casual mention to actively warn friends and family, post publicly, or both. Nearly 12% will simultaneously warn people in person AND post on social media — creating dual-channel reputation damage from a single communication failure.

What This Reveals

Every communication failure is a reputation event with multiplier effects. The 7% who would stay silent are the exception. The remaining 93% will share the experience — and the majority will do so with intent. They're not casually mentioning it over dinner. Thirty-five percent will actively warn people. Eleven percent will post publicly. And 12% will do both, creating dual-channel amplification that reaches personal networks and public platforms simultaneously.

The math is unforgiving. A single dropped call or garbled connection during a stressful interaction generates, on average, multiple negative impressions across multiple channels. The reputational damage isn't linear—it's exponential. And unlike a service failure, which can be resolved with a callback or a credit, a social media reputation event is permanent, searchable, and uncontrollable.

- 93% will share a stressful communication failure. Only 7% stay silent.
- 58% will actively warn others or go public — this is intentional reputation damage, not casual venting.
- 12% will warn people personally AND post publicly, creating dual-channel amplification from a single failure.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that eliminate stressful communication failures don't just retain individual customers — they prevent the exponential reputational damage that a single failure can cause across personal and public networks.

Risk:

- Every communication failure multiplies reputational damage. A single stressful experience with a dropped call or garbled audio reaches an average of multiple contacts across personal conversations, social media, and review platforms. The cumulative brand damage dwarfs the cost of the infrastructure investment that would have prevented it.

Action:

- Quantify the reputation cost of communication failures. Multiply each failure by the sharing rate (93%), the active-warning rate (58%), and the dual-channel rate (12%) to calculate the true cost of infrastructure underinvestment.
- Invest in infrastructure that eliminates the stressful communication experiences that trigger the word-of-mouth engine — dropped calls, garbled audio, silent holds, and failed transfers.
- Monitor social media and review platforms for communication-related complaints as an early-warning system for infrastructure degradation.

Final Thought

The negative word-of-mouth engine runs on communication failures. It doesn't need a product defect, a billing error, or a service outage to activate. A single dropped call during a stressful moment is enough to trigger a cascade that reaches dozens of people across multiple channels. The only way to shut down the engine is to eliminate the fuel ,and the fuel is infrastructure failure.

Why You Need Avaya Nexus

Framing the Experience:

This data quantifies the reputation multiplier of communication failure.
The organizations that protect their brand are those that:

- Recognize that every communication failure is a reputation event — not an isolated incident
- Invest in infrastructure that eliminates the triggers: dropped calls, garbled audio, silent holds, and failed transfers
- Measure the full cost of failure — not just the lost call, but the cascade of negative impressions it generates

Empowering the Critical Communications Mindset:

- A mission-critical mindset treats every call as a reputation event with multiplier effects.
- With Avaya Nexus™, organizations deploy zea-ro-down-downtime, high-fidelity voice infrastructure that eliminates the communication failures that 93% of consumers experience protecting the brand at the infrastructure level, where it matters most.

How the Data Maps to Experience Shifts

From	To
Communication failures as isolated incidents	Communication failures as reputation events with multiplier effects
Measuring the cost of a single lost call	Measuring the cascading reputation damage across networks
Brand protection through marketing and PR	Brand protection through infrastructure reliability
Silent failures that "nobody notices."	Failures that 93% of consumers amplify across personal and public channels

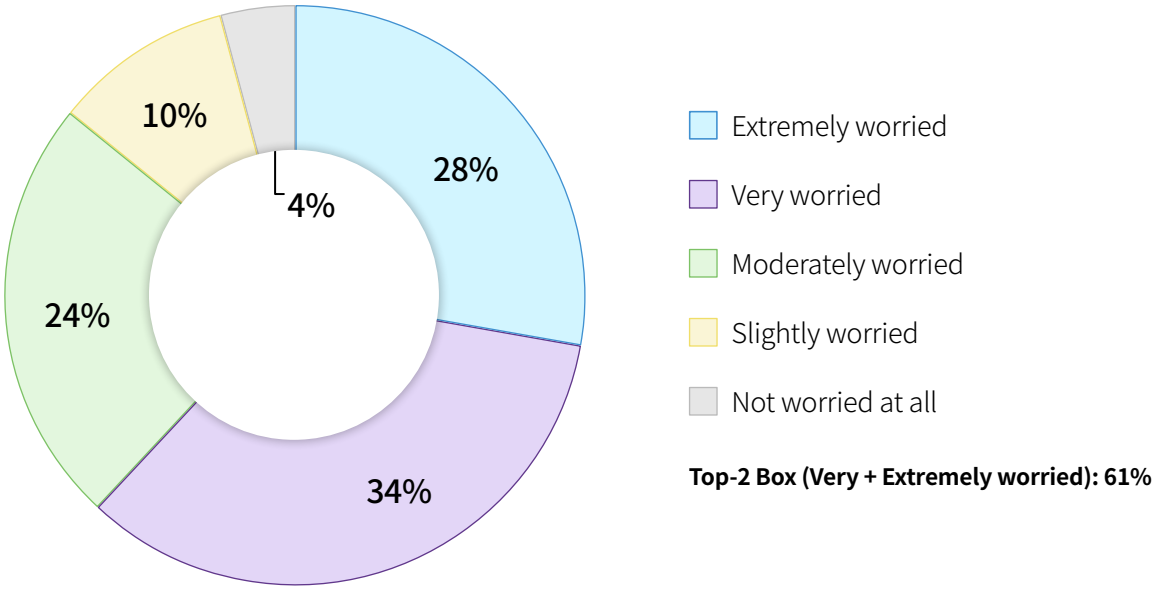
Takeaway for the C-Suite

93% of consumers will share a stressful communication failure. 58% will actively warn others or go public. 12% will do both simultaneously. This means every dropped call, every garbled connection, every silent hold is not a single incident — it is a reputation event with exponential amplification. The cost of a communication failure isn't the lost call. It's the cascade. Avaya Nexus™ delivers the zero-downtime, high-fidelity infrastructure that prevents the failures that feed the word-of-mouth engine — because in the age of social amplification, the cheapest reputation insurance is an infrastructure that never fails.

14: The Public Safety Anxiety Index — 61% Are Worried Lives Are at Risk

Question:

How worried are you that communication system failures could put lives at risk during emergencies, natural disasters, or critical healthcare situations?



Top-2 Box (Very + Extremely worried): 61%

Key Insight

61% of Americans are very worried that communication system failures could cost lives during emergencies, natural disasters, or critical healthcare situations. Only 4% are not worried at all. This is not a technology concern. It is a public safety crisis perceived by a supermajority of the population.

What This Reveals

This finding elevates the conversation from IT procurement to public safety governance. Six in ten consumers express high levels of worry — not mild concern, not theoretical unease, but active worry — that communication systems will fail when lives are on the line.

The 4% who are "not worried at all" are a rounding error. The 24% who are "moderately worried" represent a middle tier that has not yet reached high anxiety but is far from reassured. Combined with the 61% top-2-box rate, the data show that 96% of consumers have some level of concern about communication reliability in life-threatening situations.

Decision-makers who treat communication infrastructure as a routine technology purchase are misreading the stakes as perceived by the public they serve. The consumer views communication resilience as a matter of life and death, and 61% are worried the system will fail when it counts.

- 61% of consumers are very worried that communication failures could put lives at risk. Only 4% are unconcerned.
- This is not a technology anxiety — it is a public safety anxiety with direct implications for institutional accountability.
- The 24% "moderately worried" represent a cohort whose anxiety will intensify with every publicized failure and subside only with demonstrated infrastructure resilience.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that can demonstrate — not just claim — resilient communications infrastructure during emergencies position themselves as public safety leaders. This is a positioning that transcends product marketing and enters the domain of institutional trust.

Risk:

- A single publicized communication failure during an emergency — a hospital unreachable during a natural disaster, a 911 system overwhelmed during a crisis — confirms the worry that 61% of the public already carries. The reputational and regulatory consequences are severe and lasting.

Action:

- Elevate communication infrastructure decisions from IT procurement to board-level risk governance. The public perceives this as a life-and-death issue, and governance should reflect that perception.
- Invest in infrastructure with demonstrated, tested resilience under crisis conditions — not just theoretical uptime guarantees under normal operations.
- Proactively communicate resilience capabilities to stakeholders and the public. The 61% anxiety exists partly because consumers have no visibility into the infrastructure protecting them.

Final Thought

The public safety anxiety index reveals a population that has already concluded what many decision-makers have not: communication infrastructure is life-safety infrastructure. The 61% who are very worried are not overreacting. They are responding rationally to a world where emergencies are increasing in frequency, communications are increasingly digital, and the consequences of failure are increasingly visible. The question is not whether the public is worried. The question is whether the infrastructure justifies their worry — or resolves it.

Why You Need Avaya Nexus

Framing the Experience:

This data shifts the conversation about communication infrastructure from a technology discussion to a public safety discussion. The organizations that resolve the public's anxiety are those that:

- Deploy infrastructure engineered for crisis conditions — not optimized for average conditions with crisis resilience as an afterthought.
- Architect for zero downtime with Dual-Availability Zone redundancy that maintains operations through partial and complete failures
- Treat communication resilience as a public safety obligation, not a technology feature

Empowering the Critical Communications Mindset:

- A mission-critical mindset recognizes that 61% of the public is already worried about communication system failures during emergencies. The infrastructure decision either confirms that worry or resolves it.
- With Avaya Nexus™, organizations deploy the zero-downtime, carrier-grade voice architecture that resolves the public safety anxiety — because the platform was engineered for the exact scenarios that 61% of the public is worried about: the emergency, the natural disaster, the critical healthcare moment when the call cannot fail.

How the Data Maps to Experience Shifts

From	To
Communication infrastructure as an IT procurement decision	Communication infrastructure as a public safety governance decision
Uptime as a technical SLA	Resilience as a life-safety obligation
Consumer concern as abstract anxiety	Consumer concern as a measurable public safety index
Infrastructure investment justified by cost savings	Infrastructure investment justified by life-safety risk reduction

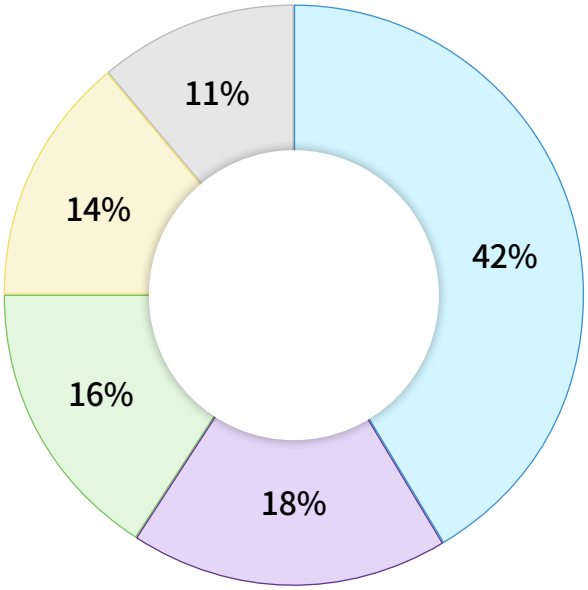
Takeaway for the C-Suite

61% of Americans are very worried that communication failures could cost lives. Only 4% are unconcerned. This is not an IT issue — it is a public safety issue that belongs on the board's risk register, not the IT department's procurement queue. CIOs and boards in healthcare, emergency services, utilities, and government must treat communication infrastructure as life-safety infrastructure — and invest accordingly. Avaya Nexus™ delivers the zero-downtime, crisis-grade architecture that resolves the anxiety 61% of the public already carries — because when the emergency hits, the infrastructure either saves or fails. There is no middle ground.

15: The Liability Assignment — Everyone Is on the Hook

Question:

If a hospital's phone system goes down during an emergency and patient care is delayed, who should be held primarily legally liable?



- Both the hospital leadership and the telecom vendor share responsibility
- The hospital's executive board
- The hospital's telecom vendor
- The hospital's IT director
- No one, technology fails sometimes

Vendor bears some liability (vendor alone + shared): 58%.
Hospital leadership bears some liability (board + shared): 60%

Key Insight

Consumers say everyone is on the hook. 60% hold hospital leadership liable, and 58% hold the telecom vendor liable when phone systems fail during an emergency. The single largest response — 42% — is shared responsibility. Only 11% accept that technology simply fails sometimes. The public does not let anyone off the hook.

What This Reveals

This is a dual-accountability finding. The vendor cannot hide behind the customer, and the customer cannot hide behind the vendor. Both are on the hook in the court of public opinion — and, increasingly, in the court of law.

The 42% who assign shared responsibility represent the dominant public sentiment: when a hospital phone system fails during an emergency and patient care is delayed, the public holds both the institution that chose the vendor and the vendor that built the platform equally accountable. The 18% who singled out the hospital's executive board are making an even more pointed judgment: the leadership team that approved the infrastructure budget is personally responsible for the outcome.

Only 11% accept that technology simply fails sometimes. This is the "acts of God" defense — and the public has overwhelmingly rejected it. In the consumer's mind, a phone system failure during an emergency is not a random event. It is a preventable failure caused by decisions made by someone — or multiple someones.

- 60% hold hospital leadership accountable. 58% hold the telecom vendor accountable. The liability is shared, not deflected.
- 42% — the single largest cohort — say both share responsibility. The vendor-selection decision and the vendor's product are coequal in the public's liability assignment.
- Only 11% accept that technology fails sometimes. The "acts of God" defense has been rejected by 89% of the public.

Implications for Building Critical Communications Infrastructure

Opportunity:

- For vendors, this data is a credibility asset. Organizations that can demonstrate purpose-built, mission-critical reliability reduce the liability exposure of the institutions they serve — and position themselves as the trusted infrastructure partner, not just another technology vendor.

Risk:

- For institutions, choosing a vendor based on cost rather than resilience is a liability decision, not just a procurement decision. When the system fails during an emergency, the public will hold both the institution and the vendor accountable — and "we chose the cheapest option" is not a defense the public will accept.

Action:

- For institutional leadership: treat vendor selection for mission-critical communications as a board-level risk decision, not a procurement decision. The public holds leadership personally accountable for the outcome.
- For vendors: build and demonstrate the resilience that protects both the vendor's reputation and the institution's liability exposure. The vendor's credibility is the institution's shield.
- For both: document resilience capabilities, test them under crisis conditions, and ensure that the infrastructure can withstand the scenarios the public is most worried about.

Final Thought

The liability assignment finding is the most consequential data point for boardroom conversations. It tells the hospital CEO: your board is on the hook. It tells the telecom vendor: your platform is on the hook. And it tells the CIO who sits between them: your vendor-selection decision determines who pays when the system fails. Choosing the right vendor isn't a technology preference. It is a liability management strategy.

Why You Need Avaya Nexus

Framing the Experience:

This data reframes vendor selection as a liability decision. The organizations that reduce their exposure are those that:

- Choose vendors with demonstrated, purpose-built resilience for mission-critical environments — not vendors who offer voice as a bundled feature in a general-purpose platform.
- Treat the vendor relationship as a shared-accountability partnership, where both parties are invested in zero-downtime outcomes.
- Document and test resilience capabilities so that the institutional leadership can demonstrate due diligence to regulators, boards, and the public.

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees vendor selection as a liability decision. The vendor's reliability is the institution's liability shield — or its liability exposure.
- With Avaya Nexus™, organizations choose a vendor whose entire architecture — zero-downtime design, Dual-AZ redundancy, carrier-grade SIP routing, hardened security — was purpose-built for the environments where failure triggers the dual-accountability judgment that 60% of the public is ready to render.

How the Data Maps to Experience Shifts

From	To
Vendor selection as a procurement decision	Vendor selection as a liability management decision
"Technology fails sometimes" is an acceptable defense	"Technology fails sometimes" was rejected by 89% of the public
Liability assigned to one party	Dual accountability: institution AND vendor share the hook
CIO as technology buyer	CIO is the person whose decision determines who pays

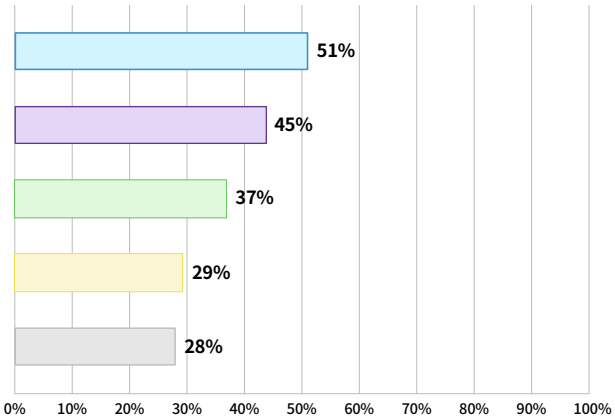
Takeaway for the C-Suite

60% of consumers hold hospital leadership liable when phone systems fail during an emergency. 58% hold the vendor liable. Only 11% accept that technology simply fails. This is a dual-accountability finding with direct implications for board-level risk governance. The vendor-selection decision is not a procurement decision — it is a liability decision. Choosing a vendor with purpose-built, mission-critical resilience is choosing the right shield. Avaya Nexus™ is that shield — engineered for zero downtime in environments where failure triggers the accountability judgment that 89% of the public is ready to deliver.

16: The Clinical Impact Chain — Poor Audio Corrupts the Data

Question:

When forced to use a garbled communication line or placed on silent hold during a medical or safety crisis, how does the poor connection affect your ability to help yourself or the patient?



- I would likely second-guess whether I heard the instructions correctly
- It would likely affect my ability to communicate facts
- I would likely exaggerate symptoms when the agent answers, just to get faster help
- I would likely hang up and attempt to call back — delaying care
- I would likely call back a second time to make sure help was correctly dispatched

(Multi-select question; percentages exceed 100%)

Key Insight

51% of consumers would second-guess medical instructions received on a garbled line. 45% say the poor connection would impair their ability to communicate facts accurately. And 37% admit they would exaggerate symptoms just to get faster attention. Poor audio doesn't just frustrate callers — it also degrades the accuracy of information exchange, introduces diagnostic distortion, and delays care delivery.

What This Reveals

This is the clinical impact chain: a single infrastructure failure cascades through every downstream process that depends on accurate voice communication.

The 51% who would second-guess instructions describe a scenario in which a patient or caregiver follows a medication dosage, a treatment protocol, or an emergency procedure based on information they aren't sure they heard correctly. The clinical risk is self-evident.

The 45% who say a poor connection would affect their ability to communicate facts are describing a scenario in which the information flowing into triage systems, medical records, and diagnostic workflows is compromised at the source — not because the caller doesn't know the facts, but because the infrastructure won't carry them clearly.

The 37% who admit they would exaggerate symptoms is the most unexpected and consequential finding. It means poor audio quality literally corrupts the clinical data flowing into triage systems. When callers inflate symptoms to compensate for a lack of trust in the connection, the downstream effects include misallocation of emergency resources, distorted clinical records, and diagnostic decisions based on artificially escalated presentations. This is not a customer experience problem. It is a clinical integrity problem.

- 51% would second-guess medical instructions over a garbled line — increasing medication, treatment, and procedural risks.
- 45% say the poor connection would impair their ability to communicate facts, corrupting the data at the source.
- 37% would exaggerate symptoms to get faster help — introducing diagnostic distortion that cascades through triage and resource allocation.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that deliver crystal-clear voice infrastructure protect the integrity of every clinical, financial, and operational data flow that depends on voice communication — turning infrastructure into a data-quality guarantee.

Risk:

- Poor audio infrastructure introduces systemic data corruption: second-guessed instructions, impaired fact communication, exaggerated symptom reporting, and redundant callbacks that waste resources and delay care. The degradation is invisible in the phone system's metrics but devastating in clinical outcomes.

Action:

- Treat voice infrastructure as a data-integrity tool. Every clinical decision, triage assessment, and emergency dispatch that depends on voice communication is only as accurate as the audio carrying it.
- Deploy high-fidelity, wideband audio infrastructure that preserves every word, every nuance, and every factual detail — especially in environments where the information exchanged on the call feeds downstream clinical, financial, or operational systems.
- Audit the clinical impact chain: trace the path from the caller's voice through the phone system into the triage workflow, the medical record, and the dispatch system. Identify every point where audio degradation introduces data corruption.

Final Thought

The clinical impact chain reveals that voice infrastructure is not just a communications tool — it is a data pipeline. Every clinical instruction delivered over voice, every symptom reported by a caller, every fact communicated during a crisis flows through the phone system before it reaches the professional, the record, or the AI. When the audio degrades, the data degrades. When the data degrades, the decisions degrade. The chain is only as strong as the voice infrastructure at its foundation.

Why You Need Avaya Nexus

Framing the Experience:

This data reveals that voice infrastructure is clinical infrastructure. The organizations that protect data integrity are those that:

- Deploy carrier-grade, high-fidelity voice that preserves every word and every nuance — so callers don't second-guess, professionals don't misinterpret, and AI systems don't process garbage input.
- Recognize that the 37% exaggeration finding means poor audio doesn't just degrade the call — it actively corrupts the clinical data flowing downstrea.m
- Treat voice quality as a first-order input to AI accuracy, triage integrity, and clinical decision-maki.ng

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees voice quality as data quality. The audio fidelity of the connection determines the accuracy of every system that depends on it.
- With Avaya Nexus™, organizations deploy the high-fidelity voice infrastructure that protects the clinical impact chain — because the platform delivers the audio clarity that AI-driven transcription, sentiment analysis, and real-time keyword detection depend on. When the voice is clear, the data is clean. When the data is clean, the decisions are sound. Avaya Nexus™ is the foundation that makes the entire chain trustworthy.

How the Data Maps to Experience Shifts

From	To
Voice quality as a caller experience metric	Voice quality as a clinical data integrity metric
Audio degradation as an inconvenience	Audio degradation as systemic data corruption
Symptom reporting as a reliable input	Symptom reporting distorted by infrastructure quality (37% exaggeration)
AI accuracy as an algorithm problem	AI accuracy as an infrastructure problem — garbage in, garbage out

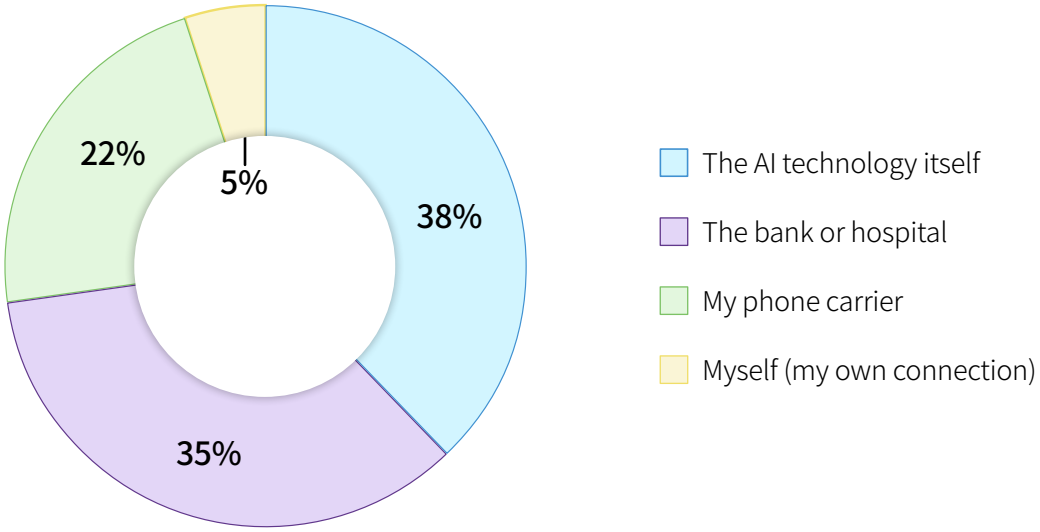
Takeaway for the C-Suite

51% of consumers would second-guess medical instructions on a garbled line. 37% would exaggerate symptoms to get faster help. This means poor voice infrastructure doesn't just degrade the caller experience — it corrupts the clinical data that feeds triage, diagnosis, and AI systems. For healthcare, financial services, and emergency services CIOs, voice quality is data quality. Every AI investment, every clinical workflow, every triage system is only as accurate as the audio infrastructure beneath it. Avaya Nexus™ delivers the high-fidelity, carrier-grade voice that protects the entire data chain — because in mission-critical environments, the call quality IS the data quality.

17: The AI Blame Attribution — Only 5% Blame Themselves

Question:

If an automated AI system at your healthcare provider or bank misinterprets your information — for example, getting a medication dosage or account number wrong — because the phone connection was poor, who do you hold most responsible for the error?



Key Insight

73% of consumers blame either the AI or the institution when AI gets it wrong due to poor audio, and only 5% blame themselves. The blame splits almost evenly between the AI technology (38%) and the institution deploying it (35%), meaning organizations that deploy AI-powered voice systems on poor infrastructure face dual reputational exposure: the AI and the brand take a hit.

What This Reveals

The 5% self-blame figure is the most striking finding in the entire AI section. Consumers categorically refuse to accept personal responsibility for infrastructure-driven AI errors. They don't think, "My connection was bad, so the AI misheard me." They think, "the bank's system got my information wrong, and someone should answer for it."

The even split between AI blame (38%) and institution blame (35%) tells a nuanced story. It means deploying AI on poor infrastructure creates dual reputational exposure. The consumer doesn't just lose confidence in the AI — they lose confidence in the institution that chose to deploy it without ensuring the underlying audio was good enough to feed it accurate data. The AI and the brand are judged together.

The 22% who blame the phone carrier is a secondary but significant finding: it means the infrastructure ecosystem itself — not just the application layer — is being evaluated by consumers. But the dominant judgment falls on the AI and the institution. The consumer's message is clear: if you deploy AI, you own the outcome. And if the outcome is wrong because the audio was bad, you should have fixed the audio first.

- 73% blame the AI or the institution. Only 5% blame themselves. Consumers refuse to own infrastructure-driven AI errors.
- The 38/35 split between AI blame and institution blame means dual reputational exposure: the technology and the brand are judged together.
- Deploying AI on poor voice infrastructure doesn't just produce poor outputs — it creates a blame attribution that damages both the AI's credibility and the institution's reputation.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that invest in high-fidelity voice infrastructure before deploying AI-powered voice applications create a clean data foundation that protects both the AI's accuracy and the institution's reputation. Infrastructure quality becomes the AI's credibility shield.

Risk:

- Deploying AI on degraded audio infrastructure is a compounding liability. The AI produces errors because the input is corrupted, the consumer blames both the AI and the institution, and the organization's investment in AI — which was supposed to improve service — becomes a reputational liability instead.

Action:

- Sequence the investment correctly: fix the voice infrastructure first, then deploy AI. AI accuracy depends on input quality, and input quality depends on the audio infrastructure.
- Treat high-fidelity voice as an AI prerequisite, not an AI enhancement. No amount of algorithmic sophistication compensates for garbled input.
- Measure AI error rates by audio quality tier. Quantify the correlation between connection quality and AI accuracy to build the business case for infrastructure investment.

Final Thought

The AI blame attribution finding delivers a message that every CIO deploying voice-based AI needs to hear: the consumer holds you responsible for AI errors, even when the root cause lies in the audio infrastructure that feeds the AI. Fixing the algorithm without fixing the audio is like tuning a race car engine and leaving the fuel line clogged. The AI is only as good as the voice infrastructure beneath it — and when it fails, the consumer blames everything above the infrastructure: the AI, the institution, and the decision-maker who deployed both without ensuring the foundation was sound.

Why You Need Avaya Nexus

Framing the Experience:

This data confirms that AI quality is infrastructure quality. The organizations that protect their AI investments are those that:

- Deploy high-fidelity voice infrastructure as the foundation for every AI-powered voice application.
- Recognize that AI accuracy depends on audio clarity — and that degraded audio produces degraded outputs that the consumer will blame on the institution
- Treat voice infrastructure as the AI's first and most critical dependency, not as a separate system managed by a separate team.

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees voice infrastructure as the AI's data pipeline. Clean audio in, accurate AI out. Garbage audio in, reputational damage out.
- With Avaya Nexus™, organizations deploy the high-fidelity voice infrastructure that underpins AI-driven transcription, real-time keyword detection, voice authentication, and sentiment analysis. The platform delivers the audio clarity that turns AI from a liability into an asset — because when the voice is clear, the AI is accurate. When the AI is accurate, the institution's reputation is protected.

How the Data Maps to Experience Shifts

From	To
AI errors are blamed on the algorithm	AI errors are blamed on the institution that deployed it
Voice infrastructure and AI as separate investments	Voice infrastructure is the AI's first dependency
"The AI got it wrong."	"The institution deployed AI on bad infrastructure."
Self-blame for connection quality	Consumer refusal to accept responsibility (only 5%)

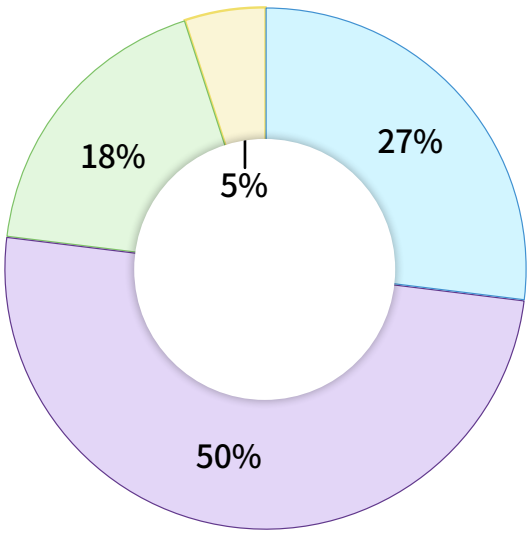
Takeaway for the C-Suite

73% of consumers blame the AI or the institution when AI gets it wrong because of poor audio quality. Only 5% blame themselves. This means that every AI deployment on degraded voice infrastructure carries dual reputational risks — the AI loses credibility, and the brand loses trust. CIOs must sequence the investment correctly: high-fidelity voice infrastructure first, AI deployment second. Avaya Nexus™ delivers the carrier-grade audio foundation that AI-powered applications require — because in mission-critical environments, AI accuracy is not an algorithm problem. It is an infrastructure problem.

18: The Emotional Fidelity Requirement — 76% Say Emotional Tone Is Critical

Question:

When you are reporting an emergency over the phone, how important is it that the representative can hear the subtle emotions in your voice (like a sigh, a hesitation, or the shakiness of your breath), rather than just the literal words you are speaking?



Top-2 Box (Very important + Absolutely critical): 76%

Key Insight

76% of consumers say it is critical that emergency responders can hear their emotional tone — not just their words. The concentration at "Very important" (50%) as the clear plurality is particularly powerful: consumers aren't casually agreeing, they're affirming at high intensity. Only 5% say it doesn't matter. Voice fidelity is not a luxury. It is a clinical requirement.

What This Reveals

This finding redefines what "voice quality" means in a mission-critical context. It is not just about audibility — can the agent hear the words? It is about emotional fidelity — can the agent hear the sigh, the hesitation, the tremor in the voice that signals distress beyond what the words convey?

Compressed, low-bitrate audio strips out the paraverbal signals — the breath, the cadence, the vocal tremor — that professionals use to assess severity, detect distress, and calibrate response urgency. A triage nurse who hears the words "I'm fine" but can also hear the shakiness in the caller's breath knows the patient is not fine. A dispatcher who hears the words "I think someone broke in" but also hears the whispered, controlled terror in the caller's voice calibrates the response differently than if the words came through flat and compressed.

High-fidelity voice isn't a premium feature. It is a clinical and operational tool. The 76% finding validates every investment in HD voice, wideband audio, and carrier-grade voice infrastructure — not because consumers want a better-sounding phone call, but because they need the professional on the other end to hear what they can't put into words.

- 76% say it is critical that the representative can hear their emotional tone during an emergency. This exceeded pre-survey projections of 65%.
- The 50% plurality at "Very important" reflects high-intensity affirmation — not casual agreement.
- Emotional fidelity is a clinical tool: the paraverbal signals stripped by compressed audio are the signals professionals depend on to assess severity, detect distress, and calibrate response.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that invest in high-fidelity, wideband voice infrastructure give their frontline professionals a clinical advantage: the ability to hear what the caller can't say. This transforms voice infrastructure from a communications utility into a diagnostic tool.

Risk:

- Compressed, low-bitrate audio doesn't just reduce sound quality — it strips the emotional data that professionals use to assess the true severity of a situation. The cost is not a degraded caller experience. It is a degraded clinical or operational assessment with downstream consequences for care delivery, emergency response, and resource allocation.

Action:

- Deploy a wideband, high-fidelity audio infrastructure that preserves the full frequency range of the human voice — including paraverbal signals that convey emotional content.
- Train frontline professionals to leverage emotional fidelity as a diagnostic and assessment tool — and ensure the infrastructure beneath them supports that training.
- Evaluate voice infrastructure not just on audibility metrics (can the words be heard?) but on fidelity metrics (can the emotion be heard?).

Final Thought

The emotional fidelity requirement reveals a dimension of voice quality that most infrastructure evaluations miss entirely. It isn't about whether the caller's words reach the professional. It's about whether the caller's emotional state reaches the professional. The sigh. The hesitation. The shakiness. These aren't background noise — they are clinical data. And 76% of consumers are counting on the infrastructure to carry them.

Why You Need Avaya Nexus

Framing the Experience:

This data confirms that voice fidelity is not a premium feature — it is a clinical and operational requirement. The organizations that harness emotional fidelity are those that:

- Deploy carrier-grade, high-fidelity voice infrastructure that preserves the full emotional bandwidth of the human voice
- Recognize that the paraverbal signals — sighs, hesitations, vocal tremors — are clinical data that professionals depend on
- Treat audio fidelity as an input to AI sentiment analysis, real-time emotion detection, and clinical triage — not just as a caller experience metric

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees voice fidelity as emotional fidelity. The audio quality determines whether the professional hears words alone or hears the human being behind them.
- With Avaya Nexus™, organizations deliver the high-fidelity voice that preserves every emotional signal — because the platform's carrier-grade audio is engineered to carry not just the caller's words, but their fear, their urgency, and their need to be understood. And as voice increasingly feeds AI-powered sentiment analysis and real-time transcription, that fidelity becomes the foundation for every intelligent system that sits on top of it.

How the Data Maps to Experience Shifts

From	To
Voice quality measured by audibility	Voice quality measured by emotional fidelity
"Can the words be heard?"	"Can the emotion be heard?"
Compressed, low-bitrate audio is cost-efficient	Compressed audio as clinical data loss
HD voice as a premium feature	HD voice as a clinical and operational requirement

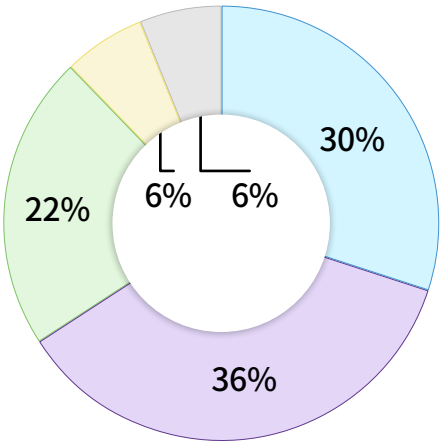
Takeaway for the C-Suite

76% of consumers say it is critical that emergency responders can hear their emotional tone — not just their words. This redefines voice quality from an audibility metric to a fidelity metric. For healthcare, emergency services, and financial services CIOs, the implication is direct: compressed audio strips the emotional data that professionals use to assess severity, detect distress, and save lives. High-fidelity voice infrastructure is not a premium upgrade. It is a clinical tool. Avaya Nexus™ delivers carrier-grade audio fidelity engineered for the environments where hearing the sigh, the hesitation, and the tremor isn't a nice-to-have — it's the difference between an accurate assessment and a missed signal.

19: The Platform Substitution Rejection — 88% Are Concerned, Only 6% Welcome the Switch

Question:

Some businesses are considering replacing their dedicated phone systems with the same voice technology used in video conferencing platforms (such as Zoom or Teams). If your bank, hospital, or utility company made this switch, how would you feel?



- Extremely concerned
- Very concerned
- Slightly concerned
- I'd welcome this change; video conferencing voice quality is good enough
- Not concerned

Any concern (Slightly + Very + Extremely): 88%
High concern (Very + Extremely): 66%

Key Insight

88% of consumers are concerned that banks and hospitals will replace dedicated phone systems with video conferencing technology. Two-thirds are very concerned. Only 6% would welcome the switch. This is direct consumer rejection of the platform-substitution thesis: purpose-built, carrier-grade voice infrastructure for critical services is not interchangeable with collaboration-platform voice. Consumers understand the difference even when procurement spreadsheets don't.

What This Reveals

This is the single most powerful data point for every competitive conversation against the UCaaS-for-everything strategy. The 88% concern rate exceeded pre-survey projections of 76% — indicating consumer rejection of platform substitution is even stronger than anticipated.

The 6% welcome rate is devastating for the substitution narrative. For every 100 consumers served by a hospital or bank, only 6 would be comfortable with the switch to video-conferencing-grade voice. The remaining 94 are either concerned (88%) or indifferent (6%) — and indifference is not endorsement.

The concentration at "Very concerned" (36%) and "Extremely concerned" (30%) reveals that two-thirds of consumers hold this view with high intensity. This is not mild unease. There is strong opposition to the idea that a general-purpose collaboration platform can serve as the voice backbone for the institutions they depend on in critical moments.

For CIOs evaluating a UCaaS-for-everything strategy in critical-service environments, this finding should be the forcing function: the consumer has spoken, and the message is clear. Purpose-built voice infrastructure and collaboration-platform telephony are not interchangeable — and 88% of the public knows it.

- 88% express concern about banks and hospitals replacing dedicated phone systems with video conferencing technology. This exceeded pre-survey projections by 12 points.
- Only 6% would welcome the change. A supermajority of the public has rejected the substitution thesis.
- 66% are very concerned — high-intensity opposition, not mild unease.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that commit to purpose-built, carrier-grade voice infrastructure for critical services can position that commitment as a direct response to consumer demand — a trust signal that differentiates them from competitors who have adopted the UCaaS-for-everything approach.

Risk:

- Organizations in critical service verticals that replace dedicated phone systems with collaboration platform voice are making a decision that 88% of their consumers oppose. The cost savings realized in IT procurement are offset by the trust deficit created in the consumer relationship.

Action:

- Evaluate voice infrastructure independently from collaboration infrastructure. The consumer sees them as fundamentally different — and so should the procurement process.
- Position the retention of purpose-built voice infrastructure as a consumer-facing commitment, not just a back-office technology decision. The 88% concern rate means this is a message consumers will respond to.
- Challenge any vendor pitch that equates collaboration-platform voice with carrier-grade mission-critical voice. The consumer has already rejected that equivalence — and the data supports them.

Final Thought

The platform substitution rejection is the clearest signal in the entire survey. Consumers are not confused about what they want. They do not believe that the voice technology powering their Tuesday morning team standup is the same technology that should power the call when their bank detects fraud or their hospital delivers test results. 88% are concerned. 66% are strongly concerned. Only 6% welcome the idea. The consumer has rendered a verdict — and the verdict is unambiguous: purpose-built voice infrastructure for critical services is not optional. It is expected.

Why You Need Avaya Nexus

Framing the Experience:

This data is the definitive consumer mandate for purpose-built critical communications infrastructure. The organizations that heed it are those that:

- Reject the platform-substitution thesis and invest in voice infrastructure purpose-built for mission-critical environments.
- Recognize that consumers understand the difference between collaboration-platform voice and carrier-grade voice — even if the procurement spreadsheet treats them as equivalent
- Position their commitment to dedicated voice infrastructure as a trust signal, not just a technology choice

Empowering the Critical Communications Mindset:

- A mission-critical mindset does not substitute. It builds purpose. Collaboration platforms serve collaboration. Mission-critical voice infrastructure serves life-safety, operational continuity, and regulated operations. The two are not interchangeable.
- With Avaya Nexus™, organizations deploy the purpose-built, carrier-grade voice platform that 88% of consumers expect — and that the remaining 6% have failed to justify replacing. Avaya Nexus™ is not a collaboration suite with a phone feature attached. It is a zero-downtime, hardened, high-fidelity voice architecture engineered for environments where a dropped call isn't a "Teams moment"—it's a crisis.

How the Data Maps to Experience Shifts

From	To
UCaaS-for-everything as the default strategy	Purpose-built voice for critical services as the consumer mandate
Collaboration-platform voice as "good enough."	Consumers are rejecting platform substitution at 88%
Voice infrastructure as a bundled feature	Voice infrastructure as an independent, mission-critical investment
Cost savings are driving the substitution decision	Consumer trust is driving the infrastructure decision

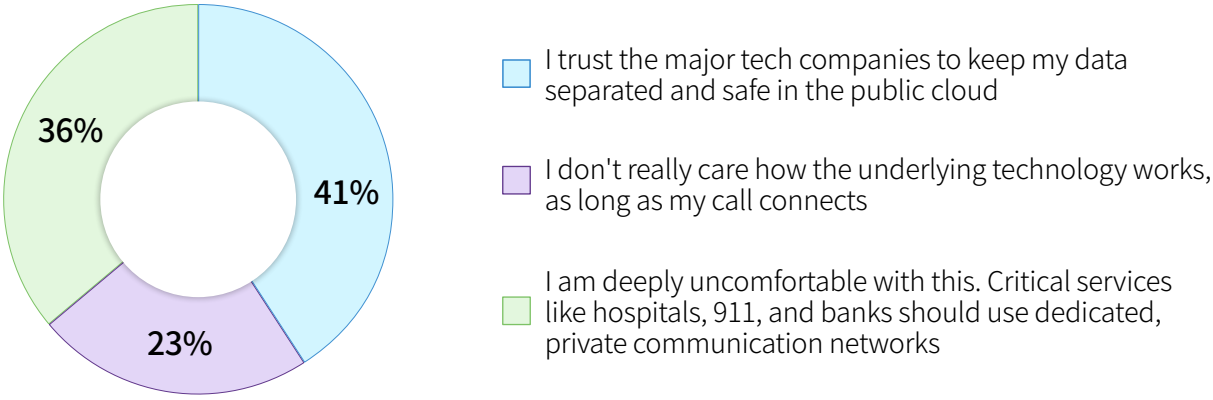
Takeaway for the C-Suite

88% of consumers are concerned that banks and hospitals will replace dedicated phone systems with video conferencing technology. Only 6% welcome the idea. This is not a technology preference — it is a consumer mandate that directly challenges the UCaaS-for-everything strategy in critical-service verticals. CIOs who substitute collaboration-platform voice for purpose-built voice infrastructure are deciding that 88% of their consumers oppose — and that 66% oppose strongly. Avaya Nexus™ is the purpose-built alternative: a zero-downtime, carrier-grade, high-fidelity voice platform engineered for the environments where the consumer has already told you that "good enough" isn't good enough.

20: The Cloud Architecture Awareness Test — 36% Are Deeply Uncomfortable

Question:

Many modern business phone systems route highly sensitive hospital and banking calls through the same "shared public cloud" servers used for retail websites, video streaming, and online gaming. Knowing this, which of the following statements do you agree with most?



Key Insight

Consumers are split on cloud infrastructure — but 36% are deeply uncomfortable with hospitals and banks sharing servers with video streaming and gaming. When combined with the 23% who are infrastructure-agnostic ("just make it work"), a majority (59%) are either concerned or indifferent to the public-cloud trust argument. Only 41% actively trust big tech to keep data separated and safe.

What This Reveals

This finding requires careful framing. It does not produce a clean majority mandate for the private cloud. But it does produce something more nuanced and arguably more useful: a substantial consumer constituency — more than one in three — that expresses active discomfort with the shared-infrastructure model for critical services.

The 41% who trust big tech are the largest single cohort, and they deserve acknowledgment. But trust is not the same as endorsement. Many of these consumers may simply lack the technical literacy to evaluate the risk, and their trust may erode rapidly after a single publicized breach or outage involving shared infrastructure.

The 23% who are agnostic represent the persuadable middle. They don't care how the technology works — they care that it works. This cohort's loyalty goes to whichever provider delivers reliability, regardless of architecture. They are not allies of the public-cloud narrative; they are allies of outcomes. And when outcomes fail on shared infrastructure, they move.

The strategic framing: 59% of consumers are either actively uncomfortable with shared cloud infrastructure or indifferent to the trust pitch that underpins it. That is not a mandate for multi-tenant public cloud in critical services. It is an opening for the hybrid, dedicated-infrastructure positioning that Avaya Nexus™ represents.

- 36% are deeply uncomfortable with critical services sharing public cloud infrastructure with consumer applications. This is a substantial minority that validates the dedicated-infrastructure thesis.
- 23% are infrastructure-agnostic — loyal to outcomes, not architecture. They are not public-cloud advocates; they are reliability advocates.
- 59% are either uncomfortable or indifferent to the public-cloud trust argument. Only 41% actively trust big tech to keep data safe in shared infrastructure.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that offer dedicated, private, or hybrid infrastructure for critical voice communications address the concerns of the 36% who are actively uncomfortable — and win the loyalty of the 23% who care only about outcomes by delivering superior reliability.

Risk:

- Organizations that deploy mission-critical voice on multi-tenant public cloud infrastructure are betting on a trust narrative that only 41% of consumers actively endorse — and that could collapse with a single publicized failure.

Action:

- Offer deployment flexibility: dedicated cloud, on-premises via hyperscalers, or hybrid models that allow organizations to match their infrastructure to their regulatory and risk requirements — not to a one-size-fits-all cloud mandate.
- Position infrastructure choice as a consumer-facing trust signal. The 36% who are uncomfortable represent a vocal, influential constituency — and their concerns align with the regulatory and compliance requirements that many critical-service organizations already face.
- Use this data as supporting texture alongside the Q20 platform-substitution rejection (88%), not as a standalone proof point. The 36% uncomfortable finding gains its full force within the broader survey narrative.

Final Thought

The cloud architecture awareness test doesn't produce a simple headline. It produces something more valuable: a nuanced picture of a public that is divided, persuadable, and increasingly aware that the infrastructure beneath their most sensitive calls matters. The 36% who are deeply uncomfortable are the canaries in the coal mine. They represent a growing consumer awareness — and that will only accelerate as data breaches, outages, and infrastructure failures make the shared-cloud model more visible to the public. The question for CIOs is not whether the public cares about cloud architecture today. It's whether they'll care tomorrow — and whether the infrastructure decision made today will survive that scrutiny.

Why You Need Avaya Nexus

Framing the Experience:

This data validates the hybrid, deployment-flexible positioning that Avaya Nexus™ delivers. The organizations that navigate the cloud-architecture divide are those that:

- Offer deployment flexibility — dedicated cloud, on-premises, or hybrid — rather than forcing a one-size-fits-all public cloud migration.
- Recognize that 36% of consumers are already uncomfortable with shared infrastructure for critical services, and that this percentage will grow as awareness increases
- Position infrastructure choice as a trust signal, aligning the organization's deployment model with its consumers''s expectations and its regulator's requirements

Empowering the Critical Communications Mindset:

- A mission-critical mindset does not force a critical voice into a shared, multi-tenant public cloud because the procurement spreadsheet says it's cheaper. It deploys infrastructure that matches the risk profile of the environment it serves.
- With Avaya Nexus™, organizations choose their deployment model — dedicated cloud, on-premises via hyperscalers, or hybrid — without sacrificing the zero-downtime reliability, hardened security, and carrier-grade voice quality that mission-critical environments demand. The platform delivers modernization with control: cloud-native architecture without forced migration to multi-tenant public cloud.

How the Data Maps to Experience Shifts

From	To
Public cloud is the default for all workloads	Deployment flexibility matched to risk profile
"Trust big tech to keep it safe" as the only narrative	36% actively uncomfortable, 23% indifferent to the trust pitch
One-size-fits-all cloud migration	Dedicated, hybrid, and on-prem options for critical voice
Infrastructure architecture is invisible to consumers	Infrastructure architecture is increasingly visible — and judged

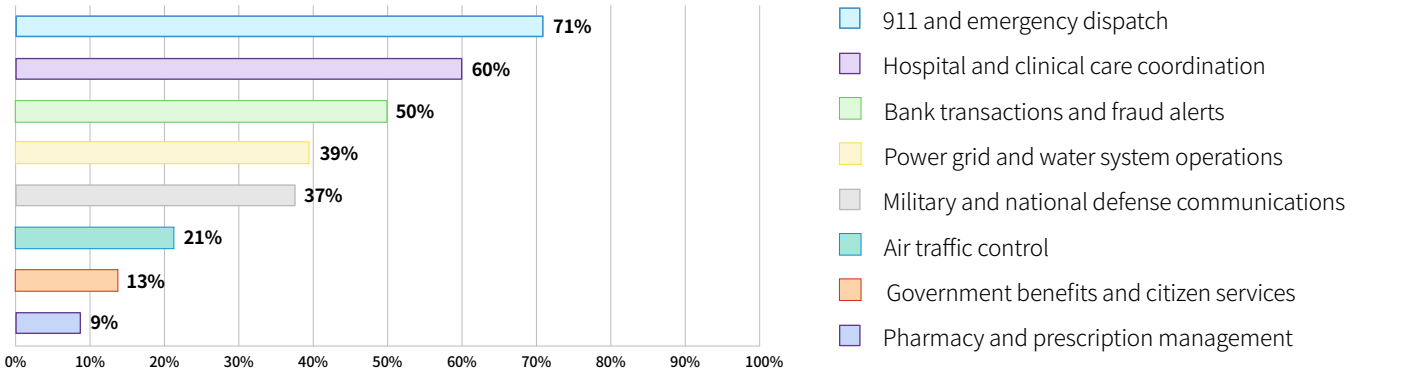
Takeaway for the C-Suite

36% of consumers are deeply uncomfortable with hospitals and banks routing sensitive calls through shared public cloud servers. Another 23% are indifferent to the cloud trust pitch — they care about outcomes, not architecture. Combined, 59% are either concerned or unpersuaded by the public-cloud narrative for critical services. This doesn't mean clouds are wrong. It means a one-size-fits-all cloud is wrong for mission-critical voice. Avaya Nexus™ delivers the deployment flexibility that this data demands: dedicated cloud, on-premises via hyperscalers, or hybrid — all on a zero-downtime, cloud-native architecture that modernizes without forcing a move to multi-tenant public cloud. The consumer isn't asking you to reject the cloud. They're asking you to be smarter about it.

21: The Zero-Failure Priority Ranking — The Consumer Mandate Maps to the Vertical Strategy

Question:

Imagine you are advising the federal government on where to invest funds to ensure voice communication systems never fail. Which three sectors should receive the highest priority for zero-failure voice infrastructure? (Select your top 3.)



(Multi-select question; respondents selected their top 3. Percentages reflect the proportion selecting each option.)

Key Insight

71% of Americans rank 911 as the #1 priority for zero-failure voice infrastructure. Hospitals (60%) and banks (50%) round out a clear top three — a distinct tier above military (37%), power grid (39%), and all other sectors. The consumer mandate for zero-failure voice infrastructure maps directly to the critical-service verticals where Avaya Nexus™ is positioned.

What This Reveals

The clarity of the top-three ranking is the headline. Emergency services, healthcare, and financial services form a distinct tier — each selected by at least half the respondents — while every other sector falls below 40%. This is not a close ranking. It is a clear, well-separated hierarchy that reflects the public's intuitive understanding of where communication failure carries the most severe consequences.

The 71% for 911 and emergency dispatch is the expected leader, but the margin is instructive. Consumers place emergency dispatch 11 points above hospitals and 21 points above banks — a ranking that reflects the immediacy and life-or-death nature of emergency response.

The 60% for hospitals confirms that the public views healthcare communications as mission-critical infrastructure, not just clinical workflow. When 60% of consumers say hospital voice systems should never fail, they are describing a standard that most general-purpose platforms cannot meet—and that most healthcare organizations have not yet invested in achieving.

The 50% for banking crosses the threshold that confirms financial services belong in the "critical infrastructure" conversation alongside emergency services and healthcare. Half the public believes bank voice systems should be engineered to be fail-safe. This is not a nice-to-have. It is a consumer expectation with direct implications for fraud management, compliance, and institutional trust.

The 39% for the power grid and 37% for the military are notable but secondary. These sectors are perceived as critical but less dependent on consumer-facing voice than the top three. Air traffic control (21%), government benefits (13%), and pharmacy (9%) round out the list — not because they are unimportant, but because consumers perceive their voice-communication dependency as lower.

- The top three — 911 (71%), hospitals (60%), banks (50%) — form a clear, well-separated tier above all other sectors.
- Every sector in the top three is selected by at least half the respondents, confirming a consumer mandate for zero-failure voice in emergency services, healthcare, and financial services.
- The ranking aligns with Avaya's vertical strategy: the public already believes these sectors require the highest-grade communication infrastructure.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations in the top three sectors — emergency services, healthcare, and financial services — can leverage the consumer mandate as a strategic asset. The public already expects zero-failure voice infrastructure in these environments. Organizations that deliver it are meeting an expectation. Organizations that exceed it are differentiating.

Risk:

- Organizations in the top three sectors that have not invested in zero-failure voice infrastructure are operating below the standard that 50-71% of the public expects. Every publicized failure in these sectors — a 911 system that crashes, a hospital phone system that goes down during a crisis, a bank fraud line that drops calls — confirms the public's worst fears and accelerates the erosion of institutional trust.

Action:

- For emergency services (71%): treat zero-failure voice infrastructure as a non-negotiable public safety mandate. Consumer expectations are absolute, and the regulatory and legal consequences of failure are severe.
- For healthcare (60%): invest in dedicated, mission-critical voice infrastructure that matches the standard consumers apply to clinical communications. General-purpose platforms are insufficient to meet the expectations of 60% of the public.
- For financial services (50%): recognize that half the public expects zero-failure voice from banks. Fraud alerts, account security, and transaction confirmations all depend on a voice infrastructure that cannot fail — and the fraud spiral (Q9) shows what happens when it does.
- For power grid, military, and all other sectors, the consumer priority ranking is lower, but the operational consequences of failure are no less severe. These sectors should invest based on operational risk, not consumer ranking,— while recognizing that public expectations are rising.

Final Thought

The zero-failure priority ranking is not just a data point. It is a consumer mandate with a street address. The public has told us exactly where zero-failure voice infrastructure matters most: 911 dispatch, hospitals, and banks. Every CIO in these three sectors should see this ranking as a direct reflection of the public expectation they are being held to. The question is not whether the public cares. The question is whether the infrastructure meets the standard the public has already set.

Why You Need Avaya Nexus

Framing the Experience:

This data validates the Avaya vertical strategy with consumer-level precision. The organizations that meet the consumer mandate are those that:

- Deploy purpose-built, zero-failure voice infrastructure in the sectors the public has identified as the highest priority: emergency services, healthcare, and financial services.
- Recognize that the consumer mandate aligns with the regulatory and operational requirements that already govern these sectors — creating a dual justification for investment
- Treat the public's priority ranking as a strategic planning input, not just a survey finding.

Empowering the Critical Communications Mindset:

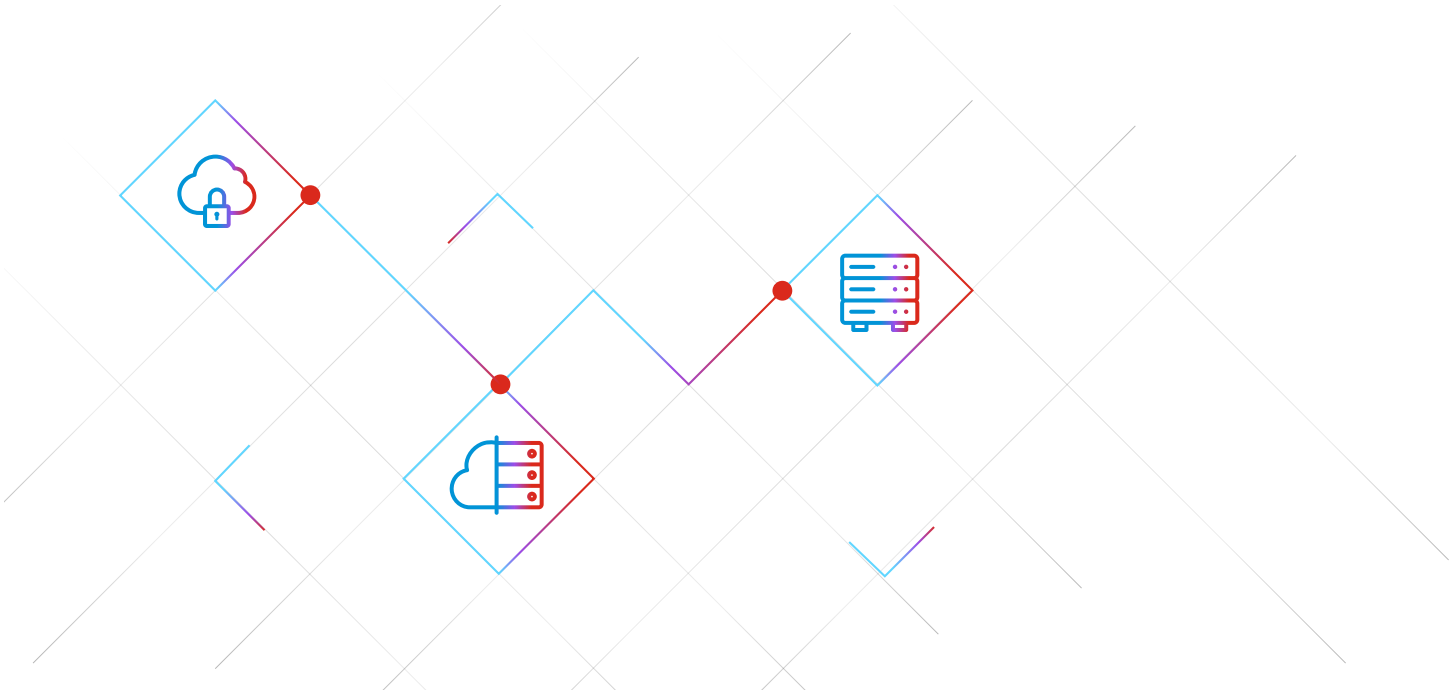
- A mission-critical mindset sees the consumer mandate as a mirror of the operational imperative. The public already knows where zero-failure voice matters most. The infrastructure should reflect that knowledge.
- With Avaya Nexus™, organizations in the top three sectors — emergency services, healthcare, and financial services — deploy the zero-downtime, carrier-grade, high-fidelity voice platform that the public expects and the mission demands. The platform's Dual-AZ architecture, hardened security, and cloud-native design are purpose-built for the environments the consumer has identified as the highest priority — because when 71% of the public says 911 must never fail, the infrastructure must be engineered to make that true.

How the Data Maps to Experience Shifts

From	To
Zero-failure voice as an aspirational goal	Zero-failure voice as a consumer mandate for the top three sectors
Infrastructure investment justified by internal metrics	Infrastructure investment justified by public expectation (71%, 60%, 50%)
Vertical strategy based on market sizing	Vertical strategy validated by consumer priority ranking
"All sectors need a good voice" as a generic pitch	Emergency services, healthcare, and financial services are the clear, consumer-identified top tier

Takeaway for the C-Suite

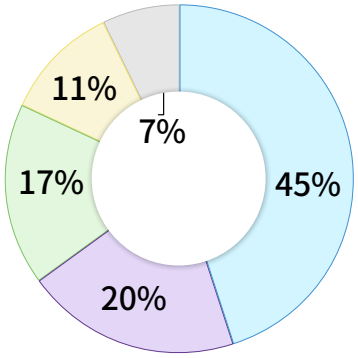
The public has named the three sectors where zero-failure voice infrastructure matters most: 911 and emergency dispatch (71%), hospitals (60%), and banks (50%). This ranking is a consumer mandate — not a suggestion. Every CIO in these three sectors should treat this data as a direct reflection of the public standard they are being held to. Avaya Nexus™ was purpose-built for exactly these environments: zero-downtime architecture, Dual-AZ redundancy, carrier-grade voice quality, and hardened security for the sectors where the consumer has already told you that failure is not an option.



22: The Shadow IT Default — 89% Have No Enterprise Backup

Question:

If your organization's official communication system goes down or becomes unusable during a critical, fast-moving incident, what would be your team's primary workaround to keep operations going?



- Bypass official channels — use personal phones/consumer apps (WhatsApp, etc.)
- Halt operations entirely and wait for IT to restore the system
- Resort to physical, manual coordination (running between departments)
- Switch to a separate, secondary backup phone system
- I don't know / I am not sure what we would do

No enterprise backup (all except secondary system): 89%

Key Insight

45% of employees would bypass official systems and use personal phones or consumer apps during a communication system failure. 20% would halt operations entirely. 17% would physically run between departments. Only 11% have access to a backup system. For 89% of organizations, the de facto disaster recovery plan for communications is either shadow IT, operational paralysis, or sheer confusion.

What This Reveals

This is the most operationally consequential finding in the survey. It reveals that, for nearly 9 in 10 organizations, the communication disaster recovery plan is not a plan at all. It is improvisation, and the improvisation defaults to the worst possible outcomes from a compliance, security, and operational continuity standpoint.

The 45% who would bypass official channels and use personal phones or consumer apps are describing shadow IT in real time. In regulated industries — healthcare, financial services, government — this improvisation is not just an operational risk. It is a compliance violation. HIPAA, PCI-DSS, SOX, and federal security mandates all have implications for sensitive communications routed through personal devices and consumer apps. A nurse coordinating patient care over WhatsApp during a system outage isn't just improvising. She is creating an unencrypted, unauditable, non-compliant communication trail in the middle of a crisis.

The 20% who would halt operations entirely are describing the cost of downtime in its most literal form: zero productivity, zero customer service, zero operational output until IT restores the system. For a hospital, that's delayed patient care. For a bank, that's frozen transactions. For an emergency dispatch center, that's unanswered calls.

The 17% who would resort to physical coordination — literally running between departments — reveal the architectural fragility beneath the digital surface. When the communication system fails, these organizations revert to pre-digital workflows: walking, shouting, and hoping.

And the 7% who don't know what they would do are perhaps the most honest. They haven't thought about it because no one has asked — and no one has planned.

- 89% of organizations have no enterprise communication backup. The disaster recovery plan is an improvisation.
- 45% would default to shadow IT — personal phones and consumer apps — creating compliance, security, and auditability violations in regulated industries.
- 20% would halt operations entirely. 17% would resort to physical, manual coordination. 7% don't know what they'd do.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that deploy resilient, zero-downtime voice infrastructure with built-in redundancy eliminate the need for shadow IT workarounds—and the compliance, security, and operational risks that come with them.

Risk:

- The shadow IT default is a compliance violation hiding in plain sight. For every regulated organization whose employees would reach for personal phones during an outage, the risk is not hypothetical. It is a single system failure away from becoming a regulatory event.

Action:

- Audit the organization's actual communication disaster recovery plan — not the documented plan, but the real one. Ask employees what they would do if the system went down today. The answers will likely mirror this survey.
- Deploy infrastructure with built-in resilience that eliminates the need for backup systems, shadow IT, or manual workarounds. Zero-downtime architecture is not a luxury — it is the only architecture that prevents the 89% improvisation scenario.
- For regulated industries, quantify the compliance exposure of the shadow IT default. Calculate the HIPAA, PCI-DSS, or SOX liability of sensitive communications routed through personal devices and consumer apps during an outage — and use that calculation to justify the infrastructure investment.

Final Thought

The shadow IT default is not a technology problem. It is an organizational resilience problem created by technology, one that only the right technology can solve. When the official communication system goes down, 89% of organizations have no enterprise backup. The employees don't wait for IT. They improvise — with personal phones, with WhatsApp, with their legs. The only way to prevent the improvisation is to prevent the outage. And the only way to prevent the outage is to deploy infrastructure engineered for zero downtime.

Why You Need Avaya Nexus

Framing the Experience:

This data shows that organizational resilience is directly a function of communication infrastructure resilience. The organizations that prevent the shadow IT default are those that:

- Deploy a zero-downtime voice infrastructure that eliminates the outage scenarios that trigger improvisation.An architect with Dual-Availability Zone redundancy so that a failure in one zone doesn't create the system-wide outage that sends employees reaching for personal phones
- Recognize that the cost of the shadow IT default — compliance violations, security breaches, operational paralysis — dwarfs the cost of the infrastructure investment that prevents it.

Empowering the Critical Communications Mindset:

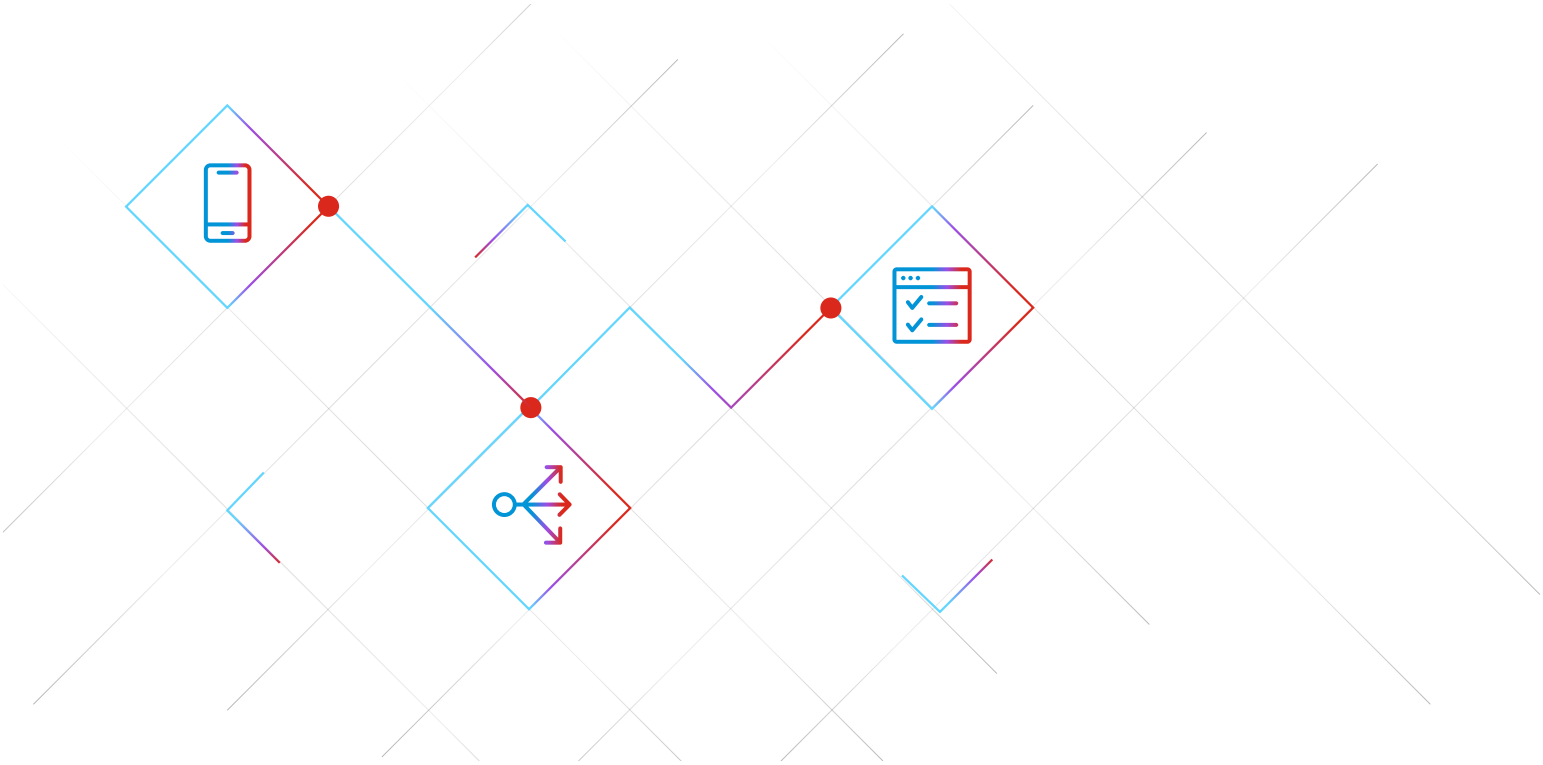
- A mission-critical mindset does not accept "we'll figure it out" as a disaster recovery plan. It engineers the infrastructure so that the disaster recovery plan is never activated — because the primary system never fails.
- With Avaya Nexus™, organizations deploy the zero-downtime, Dual-AZ architecture that eliminates the outage scenarios that 89% of organizations are unprepared for. The platform's carrier-grade resilience, containerized microservices, and seamless failover ensure that the official communication system remains operational — so employees never need to reach for WhatsApp, halt operations, or run between floors.

How the Data Maps to Experience Shifts

From	To
"We have a disaster recovery plan."	"Our employees would use WhatsApp" (45%)
Backup systems as the resilience strategy	Zero-downtime primary systems as the resilience strategy
Shadow IT as a theoretical risk	Shadow IT is the confirmed default for 45% of employees
Compliance exposure as a future concern	Compliance exposure is a single outage away from reality

Takeaway for the C-Suite

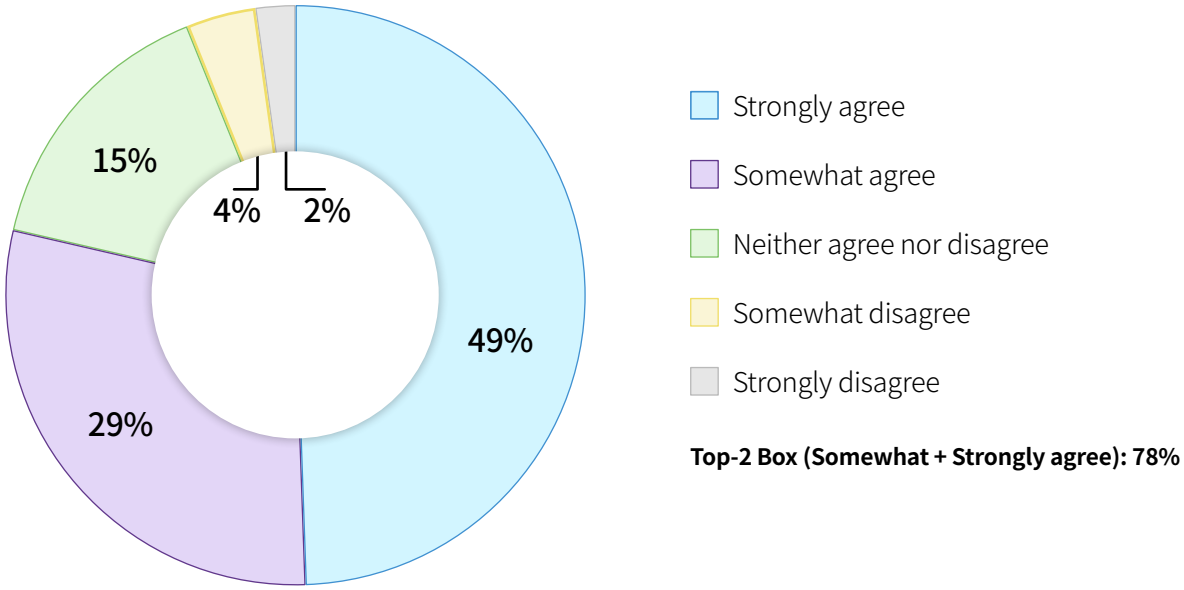
89% of organizations have no enterprise communication backup. 45% of employees would default to personal phones and consumer apps during an outage — a compliance violation in regulated industries. 20% would halt operations entirely. This is not a technology gap. It is an organizational resilience gap that sits on the CIO's desk and the board's risk register. The fix is not a backup system. The fix is a primary system that never fails. Avaya Nexus™ delivers the zero-downtime, Dual-AZ architecture that eliminates outages—and with them, shadow IT, operational paralysis, and the compliance exposure that 89% of organizations are one system failure away from experiencing.



23: The Employer Security Obligation — 78% Say It's the Employer's Responsibility

Question:

"My employer has a responsibility to invest in communication systems that are fully secure so that my data privacy is protected."



Top-2 Box (Somewhat + Strongly agree): 78%

Key Insight

78% of employees agree their employer has a responsibility to invest in secure communication systems to protect data privacy. Nearly half (49%) strongly agree. Only 7% disagree. This transforms security from an IT procurement criterion into an employee-relations obligation — a deeply held conviction, not a casual preference.

What This Reveals

The 49% "strongly agree" concentration is the anchor. When nearly half the workforce holds a conviction at the highest intensity level, it is no longer a survey response. It is an expectation with implications for employee trust, retention, and organizational culture.

Employees are not saying they would prefer secure communications. They are saying their employer has a responsibility to provide them. The language of obligation — "has a responsibility" — frames this as a duty, not a feature. Organizations that deploy consumer-grade or insufficiently secured communication platforms are not just accepting technical risk. They are violating an expectation held by more than three-quarters of their workforce.

The 15% who neither agree nor disagree are not disengaged. They are likely unaware of the security posture of their employer's communication systems, which means they haven't yet formed an opinion, not that they don't care. Once made aware, this cohort is far more likely to move toward agreement than disagreement.

For CIOs, this data shifts the security conversation from a technical evaluation to an employee-trust obligation. The question is no longer "how secure does our communication system need to be?" It is "Are we meeting the obligation that 78% of our employees believe we owe them?"

- 78% agree their employer has a responsibility to invest in secure communication systems. 49% strongly agree.
- Only 7% disagree. The conviction is near-universal and held at high intensity.
- Security is no longer an IT procurement criterion. It is an employee-relations obligation with implications for trust, retention, and culture.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that demonstrably invest in secure communication infrastructure signal to their workforce that they take the security obligation seriously — building employee trust and reinforcing the organization's commitment to data privacy.

Risk:

- Organizations that deploy insufficiently secured communication systems are not just accepting technical risk. They are violating an employee expectation held by 78% of the workforce — an expectation that, if breached, damages internal trust and creates retention risk.

Action:

- Communicate the organization's security investments to employees — not just to regulators and auditors. The 78% who hold this expectation need to know it is being met.
- Evaluate communication infrastructure security through the lens of employee obligation, not just regulatory compliance. The employee expectation may exceed the regulatory minimum.
- Deploy infrastructure with hardened security as a first-order design principle — not as a feature bolted onto a platform designed for convenience.

Final Thought

The employer's security obligation shifts the security conversation from the server room to the employee relationship. When 78% of the workforce — and 49% at the highest intensity — say the employer has a responsibility to invest in secure communications, the CIO is no longer making a technical decision. The CIO is fulfilling a trust obligation to the people who show up every day and expect that their communications, their data, and their privacy are protected by the organization they work for. Meeting that obligation is not optional. It is the price of the workforce's trust.

Why You Need Avaya Nexus

Framing the Experience:

This data reframes communication security as an obligation of employee trust. The organizations that meet this obligation are those that:

- Deploy infrastructure with hardened security validated through rigorous assessment — not self-certified claims.
- Implement modern identity and access management with role-segmented controls, Single Sign-On, and centralized authentication
- Communicate security investments to the workforce as a visible, ongoing commitment — not a background IT function.

Empowering the Critical Communications Mindset:

- A mission-critical mindset sees security not as a compliance checkbox but as an obligation to the workforce. 78% of employees say so. 49% say so strongly.
- With Avaya Nexus™, organizations deploy the hardened security posture that the workforce expects: centralized identity and access management, hardened cloud perimeter, role-segmented architecture, and security validated through static analysis and third-party assessment. The platform doesn't just meet the regulatory standard. It meets the employee standard — which, at 78%, is the standard that actually matters for organizational trust.

How the Data Maps to Experience Shifts

From	To
Security as an IT procurement criterion	Security as an employee-relations obligation
Meeting the regulatory minimum	Meeting the workforce expectation (78%)
Security investments communicated to auditors	Security investments communicated to employees
Consumer-grade communication platforms are acceptable	Consumer-grade platforms are a violation of employee trust

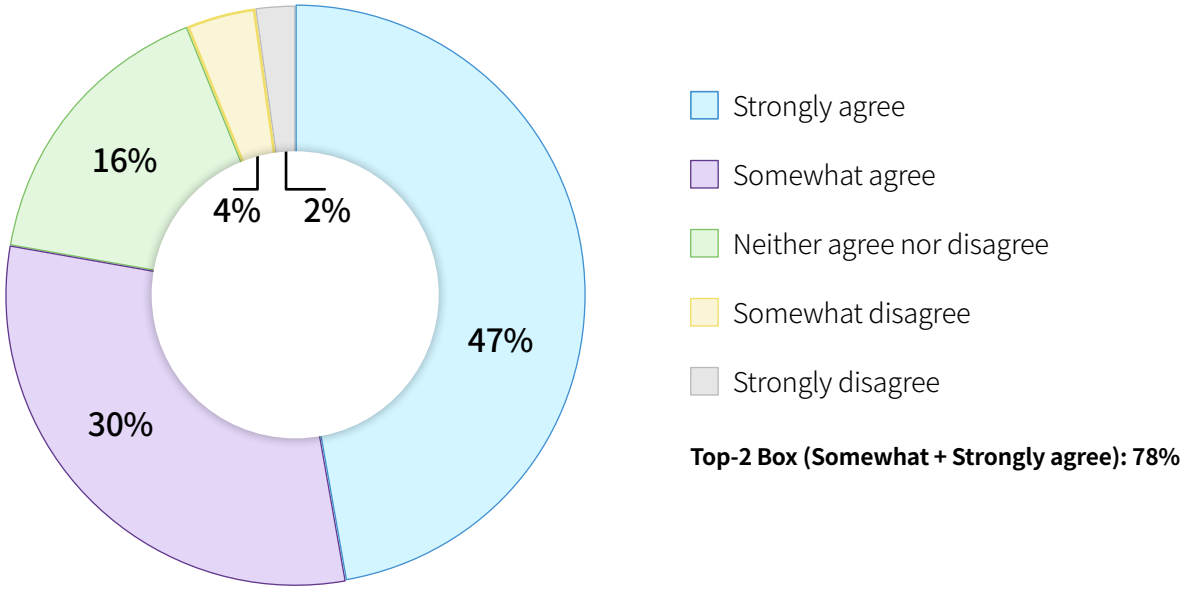
Takeaway for the C-Suite

78% of employees say their employer has a responsibility to invest in secure communication systems. 49% feel this strongly. Only 7% disagree. This is not an IT opinion — it is a workforce expectation with implications for trust, retention, and culture. CIOs who deploy insufficiently secured communication platforms aren't just accepting technical risk. They are violating an obligation held by more than three-quarters of their people. Avaya Nexus™ delivers the hardened security — centralized identity management, role-segmented access,and validated security posture — that meets both regulatory and employee standards. Because in mission-critical environments, the workforce's trust in the infrastructure is as important as the infrastructure itself.

24: The Employer Resilience Obligation — 78% Demand Crisis-Proof Communications

Question:

"My employer has a responsibility to invest in communication systems that are resilient enough to work without fail during a crisis."



Top-2 Box (Somewhat + Strongly agree): 78%

Key Insight

78% of employees say their employer must invest in crisis-resilient communications — matching the security obligation (Q24) almost exactly. The consistency is the story: employees do not choose between security and resilience. They demand both at the same intensity. For CIOs, this means resilience and security are not competing budget priorities — they are co-equal employee expectations.

What This Reveals

The Q24/Q25 symmetry is the most important analytical finding in this section. Security obligation: 78%. Resilience obligation: 78%. The numbers are virtually identical, and the intensity is virtually identical (49% strongly agree on security, 47% strongly agree on resilience). The workforce does not make a trade-off between "keep my communications secure" and "keep my communications working during a crisis." They demand both, at equal intensity, as coequal obligations of the employer.

This eliminates the false trade-off that some procurement conversations create between "secure" and "reliable." The employee perspective is unambiguous: both are required; neither is optional; and failing on either is equally unacceptable.

The 47% who strongly agree on resilience are not describing a mild preference. They are describing a deeply held expectation that the organization's communication systems will work — without fail — during the worst moments. A crisis is the test. And 78% of the workforce expects the infrastructure to pass.

- 78% agree their employer must invest in crisis-resilient communications — virtually identical to the 78% who demand security (Q24).
- 47% strongly agree. The conviction is held at nearly the same intensity as the security obligation (49%).
- Employees do not trade off between security and resilience. They are co-equal expectations, demanded at equal intensity.

Implications for Building Critical Communications Infrastructure

Opportunity:

- Organizations that deliver both security and resilience in a single platform meet the dual obligation that 78% of the workforce demands — and eliminate the false trade-off that procurement conversations often create.

Risk:

- Any infrastructure decision that prioritizes security at the expense of resilience — or resilience at the expense of security — fails to meet employee expectations on one dimension while meeting them on the other. The workforce demands both simultaneously.

Action:

- Evaluate the communication infrastructure's security AND resilience as co-equal requirements. Any platform that excels on one but compromises the other fails the 78% standard on both counts.
- Present the Q24/Q25 symmetry to leadership as evidence that the workforce has already settled the "security vs. reliability" debate. The answer is both.
- Deploy infrastructure architecturally designed to deliver both hardened security with zero-downtime resilience, not one layered on top of the other as an afterthought.

Final Thought

The Q24/Q25 symmetry is a paired finding that should be presented together — in boardrooms, in procurement evaluations, and in vendor conversations. The workforce has spoken: security and resilience are not competing priorities. They are coequal obligations. Any infrastructure that delivers one without the other is failing half the expectation —,and 78% of the workforce is keeping score on both.

Why You Need Avaya Nexus

Framing the Experience:

This paired finding validates the Avaya Nexus™ design philosophy: security and resilience are not features to be balanced. They are coequal architectural principles. The organizations that meet the dual obligation are those that:

- Deploy infrastructure where security and resilience are engineered together from the foundation — not bolted together from separate systems.
- Recognize that the employee expectation for security (78%) and resilience (78%) are identical — and that the infrastructure must meet both simultaneously
- Present the dual commitment to the workforce as a visible, organizational value — not an invisible IT decision

Empowering the Critical Communications Mindset:

- A mission-critical mindset does not choose between security and resilience. It demands both as first principles of the architecture.
- With Avaya Nexus™, organizations deploy a platform where hardened security and zero-downtime resilience are not trade-offs — they are co-equal design principles. The Dual-AZ architecture delivers resilience. The hardened cloud perimeter, centralized identity management, and role-segmented access deliver security. Both are built into the foundation, not negotiated in the procurement process. Because the workforce has already told us: 78% demand security, 78% demand resilience, and they will not accept a platform that compromises on either.

How the Data Maps to Experience Shifts

From	To
Security vs. resilience as competing budget priorities	Security and resilience as co-equal employee expectations (78% each)
Choosing one and hoping the other is "good enough."	Demanding both at full intensity
Procurement conversations that force trade-offs	Architecture that delivers both by design
Employee expectations are secondary to regulatory requirements	Employee expectations at 78% — matching or exceeding regulatory standards

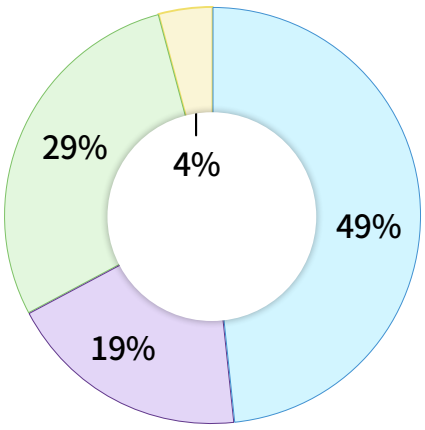
Takeaway for the C-Suite

78% of employees demand secure communications. 78% demand crisis-resilient communications. The numbers are identical. The intensity is identical. The message is identical: both are required, neither is optional. CIOs who present leadership with a platform choice that excels on security but compromises on resilience — or vice versa — are presenting a false trade-off that 78% of the workforce has already rejected. Avaya Nexus™ delivers both by design: hardened security and zero-downtime resilience as co-equal architectural principles, not competing feature priorities. Because the workforce has settled the debate. The infrastructure should reflect the verdict.

25: The Critical Services Self-Identification — The Addressable Market Is Larger Than You Think

Question:

Are you currently employed in a role that supports or delivers what you would consider a critical service — meaning a service where communication failures could significantly affect health, safety, financial security, public services, or essential operations?



- Yes, Directly
- Yes, indirectly / in a supporting role
- No
- Prefer not to answer

Critical services workforce (Direct + Indirect): 68%

Key Insight

68% of full-time employees self-identify as working in a role that supports or delivers critical services. Nearly half (49%) say they do so directly. This dramatically expands the addressable market beyond traditional definitions — healthcare, banking, emergency services — to include the supporting ecosystem of logistics, IT, administration, and operations professionals who also depend on reliable communications.

What This Reveals

The traditional definition of "mission-critical communications" draws a tight circle around a handful of verticals: hospitals, banks, 911 dispatch centers, and military installations. But the workforce itself draws a much larger circle. When asked whether their role supports or delivers a critical service — defined as one where communication failures could significantly affect health, safety, financial security, public services, or essential operations — 68% say yes.

The 49% who say they support critical services directly are the expected core: nurses, dispatchers, financial analysts, government workers, and utility operators. But the 19% who say they do so indirectly reveal the supporting ecosystem that the traditional definition misses: the IT administrator who maintains the hospital's systems, the logistics coordinator who ensures medical supplies arrive on time, the HR professional who manages benefits for a government agency. These roles depend on reliable communications just as much as the frontline — and when the communication system fails, their work is disrupted just as severely.

This finding should be used carefully. The panel is 100% employed full-time, which likely inflates the percentage relative to the general population. The 49% "directly" number is the more conservative perspective. But even at 49%, the finding suggests that the total addressable market for mission-critical communications infrastructure is significantly larger than traditional segmentation models estimate.

- 68% of full-time employees self-identify as supporting or delivering critical services. 49% do so directly.
- The traditional definition of mission-critical communications underestimates the addressable market by excluding the supporting ecosystem.
- **Note:** the employed-full-time panel composition likely inflates the percentage. The 49% "directly" stat is the more conservative figure.

Implications for Building Critical Communications Infrastructure

Opportunity:

- The addressable market for mission-critical communications infrastructure is larger than traditional segmentation suggests. Organizations that position their infrastructure investment as serving the full critical-services ecosystem — not just the narrow frontline — can justify broader deployment and capture a larger share of the supporting workforce.

Risk:

- Organizations that limit their definition of "mission-critical" to a handful of frontline roles may underinvest in the communication infrastructure serving the supporting ecosystem — leaving logistics, IT, administration, and operations professionals on consumer-grade platforms while the frontline operates on purpose-built infrastructure.

Action:

- Expand your perspective of "mission-critical communications" to include the supporting roles that 19% of the workforce identifies as indirectly critical. These roles are part of the operational chain — and a communication failure in the supporting ecosystem cascades to the frontline.
- View the 49% "directly" stat as the conservative perspective. Use the 68% combined figure for internal planning with appropriate considerations about panel composition.
- Segment the workforce by communication criticality — not by department or title — to identify where infrastructure investment will have the greatest impact on operational resilience.

Final Thought

The critical services self-identification finding is a market-sizing insight disguised as a demographic question. It tells us that the workforce has already decided what "mission-critical" means — and their definition is broader, more inclusive, and more demanding than the one used by most technology vendors and procurement teams. Two-thirds of the workforce believes they are part of the critical-services ecosystem. The infrastructure that serves them should reflect that belief.

Why You Need Avaya Nexus

Framing the Experience:

This paired finding validates the Avaya Nexus™ design philosophy: security and resilience are not features to be balanced. They are coequal architectural principles. The organizations that meet the dual obligation are those that:

- Recognize that the critical-services workforce extends well beyond the traditional frontline to include the supporting ecosystem of logistics, IT, administration, and operations.
- Deploy mission-critical voice infrastructure across the full operational chain — not just in the dispatch center or the trading floor, but in every role where a communication failure could cascade into an operational disruption.
- Use the workforce's own self-identification as a planning input for infrastructure deployment and investment prioritization.

Empowering the Critical Communications Mindset:

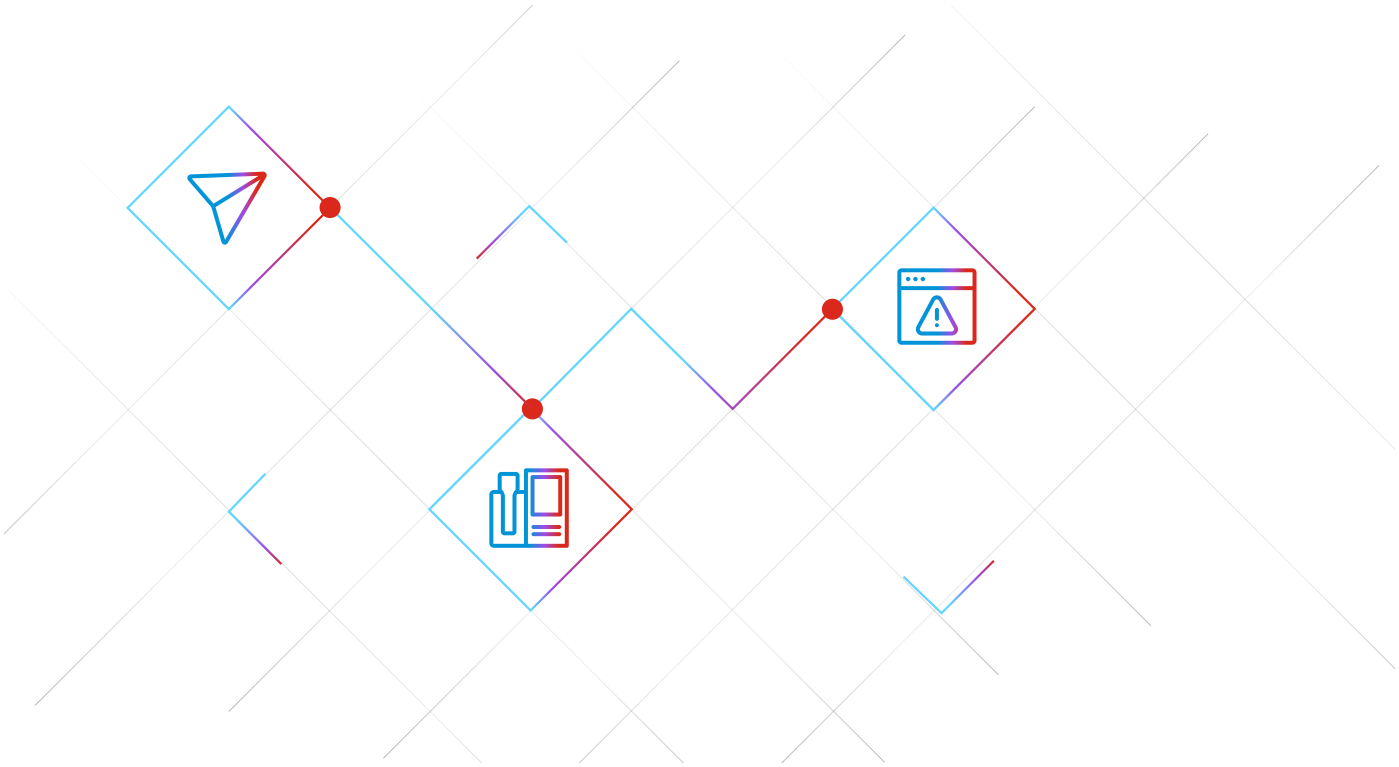
- A mission-critical mindset sees the full ecosystem, not just the frontline. When 68% of the workforce self-identifies as supporting critical services, the infrastructure must serve the full 68% — not just the traditional handful of high-profile roles.
- With Avaya Nexus™, organizations deploy a platform that scales across the full critical-services ecosystem — from the dispatch center to the administrative office, from the trading floor to the IT helpdesk. The platform's cloud-native architecture, deployment flexibility, and carrier-grade reliability ensure that every role in the operational chain is served by infrastructure engineered for the moments when communication failure is not an option.

How the Data Maps to Experience Shifts

From	To
Mission-critical communications for a narrow set of frontline roles	Mission-critical communications for the 68% who self-identify as critical
Traditional TAM based on vertical definitions	Expanded TAM based on workforce self-identification
Supporting roles on consumer-grade platforms	Supporting roles on purpose-built infrastructure
"Who needs a mission-critical voice?" answered by vendors	"Who needs a mission-critical voice?" answered the workforce itself

Takeaway for the C-Suite

68% of full-time employees self-identify as working in roles that support or deliver critical services. The traditional definition of mission-critical communications — limited to hospitals, banks, and dispatch centers — captures only a fraction of this workforce. The supporting ecosystem of logistics, IT, administration, and operations is just as dependent on reliable communications — and just as vulnerable when the system fails. CIOs should expand their definition of mission-critical to align with the workforce's, and invest in infrastructure that supports the full operational chain. Avaya Nexus™ delivers the scalable, deployment-flexible, zero-downtime architecture that serves the full 68% — because when two-thirds of the workforce says their communications are critical, the infrastructure should take them at their word.



Conclusion

What This Report Revealed

Across this research, a consistent message emerged from U.S. consumers:

Voice is non-negotiable
82% demand crystal-clear, instant connectivity with essential services — and 65% say only a human voice delivers genuine security during a crisis.

Trust is measured in seconds
57% lose faith before a silent hold hits 3 minutes. 89% say a single communication failure erodes trust. 93% will tell someone about it.

The platform substitution thesis is rejected.
88% are concerned that banks and hospitals will switch to video conferencing for voice. Only 6% welcome the idea.

AI accuracy depends on audio quality
73% blame the AI or the institution when AI errors stem from poor audio, only 5% blame themselves. 37% would exaggerate symptoms on a garbled line, corrupting the clinical data pipeline.

The public sees this as a safety issue
61% are very worried that communication failures could cost lives. 50% predict vulnerable family members would panic or give up on care entirely.

These are not passing trends. They are permanent behavioral realities. And they demand infrastructure purpose-built for reliability, clarity, and care.

Why Avaya Nexus Is the Strategic Answer

Avaya Nexus isn't a collaboration suite with a phone feature attached. It's a dedicated, mission-critical voice platform engineered for the findings in this report:

- **Zero-downtime architecture —** Dual-AZ redundancy that closes the 45% emergency confidence gap and eliminates the shadow IT default that 89% of organizations would fall back on.
- **Carrier-grade, high-fidelity voice —** Wideband audio that preserves the emotional signals 76% of consumers say are critical, and delivers the clean data that AI-powered systems depend on.
- **Hardened security —** Meeting the 78% employee expectation for secure communications as an obligation, not a feature.
- **Purpose-built for critical services —** Serving the top three sectors consumers identified for zero-failure investment: 911 (71%), hospitals (60%), and banks (50%).

From Data to Decision: What Enterprises Must Do Next

The consumer mandate is clear. To meet it, organizations must shift:

- From best-effort voice quality → to carrier-grade, deterministic voice infrastructure
- From collaboration-platform telephony → to purpose-built critical communications architecture
- From measuring uptime as a technical metric → to measuring reliability as a trust metric
- From chatbot-first escalation → to human-voice-first for high-stakes moments
- From treating security and resilience as competing priorities → to demanding both as co-equal obligations

This shift is not just about software or architecture — it's a mindset. A Critical Communications Mindset.

The Infrastructure Mandate Starts Now

Avaya Nexus gives enterprises the architecture, reliability, and intelligence to:

- Deliver what 82% of consumers demand — a voice that is always on, always clear, and always reliable
- Protect the trust that 89% of consumers are keeping score on — with every single call
- Build the infrastructure that 88% of consumers expect — purpose-built, not substituted

The consumer has rendered the verdict. The infrastructure should reflect it.

About the Survey Methodology

Quantitative Methodology

Sample: N=509

U.S. resident: Verified residents of the 50 United States and the District of Columbia

Nationally representative sample: Balanced against U.S. Census Bureau data for gender, region, and age.

18–60 years old: Strategically focused on the active workforce and primary consumer demographic.

Fielded: April 2026

Methodology

The research was conducted utilizing a sophisticated, digitally integrated consumer panel platform that leverages an **Online Non-Probability Quota Sampling** framework. Unlike traditional probability sampling, this methodology utilizes a dynamic, multi-modal recruitment engine that blends real-time **"river" sampling**—intercepting respondents as they engage with digital content—with a deep, pre-vetted **proprietary panel ecosystem**. This hybrid model ensures "freshness" while providing the precise targeting required for the 18–60 age range.

The study successfully captured a sample size of **N=509** qualified respondents through a structured 26-item survey instrument. To ensure the highest levels of data integrity, the platform employs a "Defense-in-Depth" strategy:

- **Identity Verification:** Digital fingerprinting and device hygiene protocols prevent duplicate entries by recognizing unique device metadata hashes.
- **Fraud Detection:** Real-time IP geolocation and anti-proxy technology block VPNs, while AI-driven "Reputation Scores" and honeypot fields filter out non-human bots and professional survey gamers to ensure honest data.
- **Statistical Calibration:** The dataset achieved a modeled confidence level of **95%** (with an error estimate of approximately **±4.3% to ±4.5%**) utilizing bootstrap variance estimation and post-stratification weighting (raking) to align weighted totals with U.S. Census parameters.

The provider operates under **ISO 27001 certification**, the international gold standard for Information Security, and maintains full compliance with **GDPR and CCPA** privacy regulations to ensure respondent anonymity.

About Avaya

Avaya is a global enterprise software leader that helps the world's largest organizations and government agencies forge unbreakable customer connections. The Avaya Infinity® platform is built to unify fragmented experiences, equipping enterprises to evolve their contact centers into connection centers and strengthen relationships that create business value. Learn more at **www.avaya.com**.