The State of Secure Communications 2026

88% Confident 90% Misled

Perception Gaps in Government & Critical Infrastructure

BlackBerry | Secure Communications

Contents

Introduction

Consumer messaging apps have become ubiquitous in professional settings. WhatsApp, Signal, Teams (free), and other similar platforms offer convenience, familiarity, and the promise of security through end-to-end encryption (E2EE).

However, convenience has outpaced scrutiny as communications has evolved into a target-rich environment, with this patchwork of emails and messages exposing institutions at multiple layers – app, device and network. Intelligence advisories issued by the United States and Europe in March 2026 have reinforced this reality, warning that state-backed actors are actively targeting accounts on consumer messaging platforms through phishing, impersonation and account takeover, accessing sensitive conversations without breaking encryption.

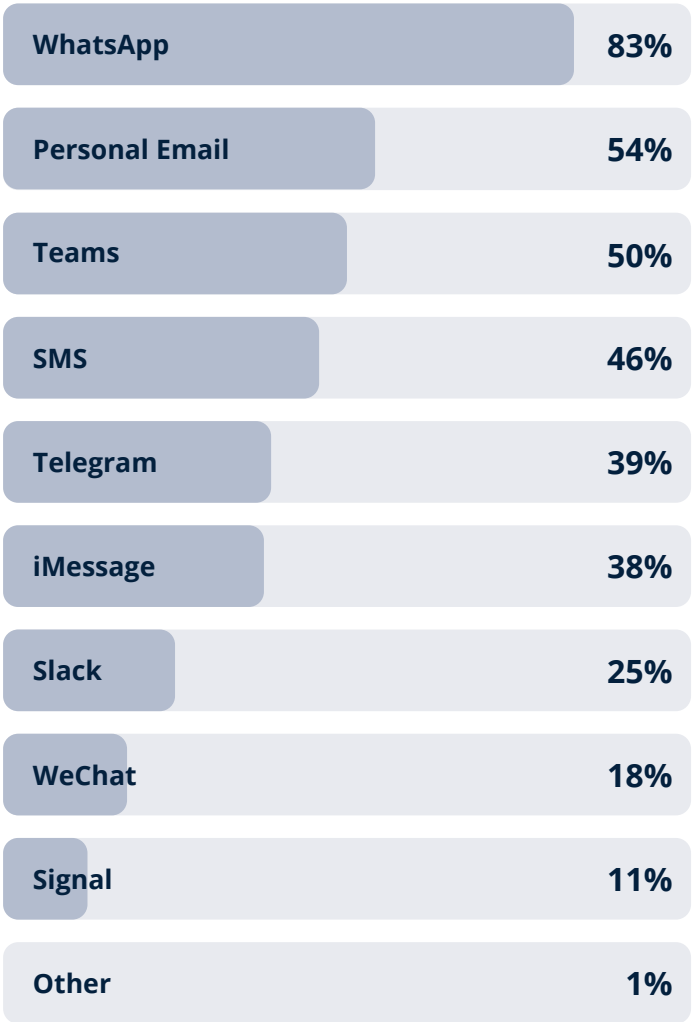
As these tools blur the lines between everyday personal use and what's required for sensitive business conversations, organizations have inherited assumptions about security that largely go unverified and bypass regular security audits. The label "encrypted" has become shorthand for "secure," obscuring important distinctions without a common understanding of what encryption actually protects.

The gap between security policy and security practice is systemic. Three in four respondents report that employees bypass approved communication tools "sometimes," "often," or "very often" for efficiency. Security policies may exist on paper, but these survey results indicate that consumer-grade apps in particular– free to download in exchange for your personal data and not built to government standards - dominate in practice.

3 in 4

respondents report that employees bypass approved communication tools "sometimes," "often," or "very often" for efficiency.

Which apps do you believe are most commonly used for important, sensitive conversations?



This survey of 700 security decision-makers across government and critical infrastructure sectors in four countries examines the gap between security perception and security reality. The findings reveal consistent patterns where organizational confidence exceeds technical capability, where security and usage policy requirements conflict with platform architecture, and where the tools chosen for sensitive communications may not deliver the protection organizations require and assume are being delivered.

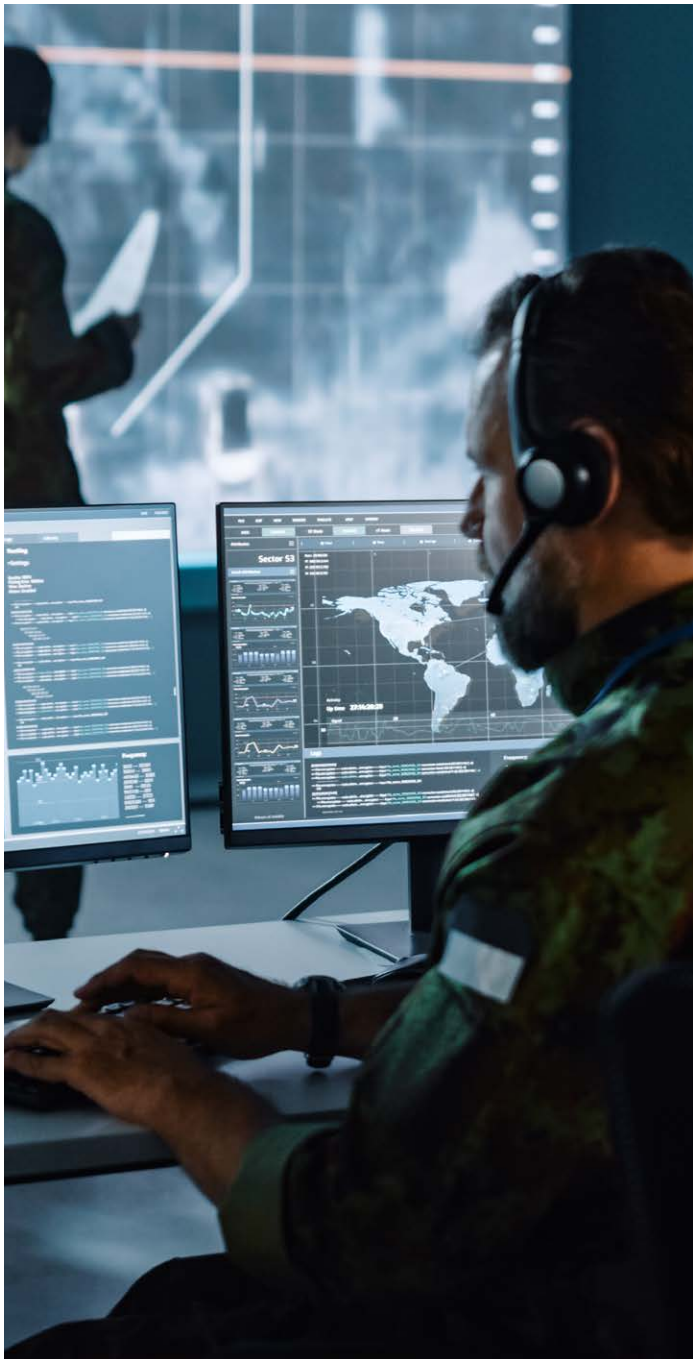
The research also examines two areas of risk that extend beyond routine secure messaging: Operational continuity in a crisis and quantum preparedness.

When critical events occur, like outages, cyber-attacks or floods, organizations need more than encrypted channels. They need unified platforms for coordinated response across teams, agencies, and jurisdictions. And as quantum computing advances, the cryptographic foundations underlying current security face a timeline threat that creates present-day vulnerability for data with long-term sensitivity.

Main drivers or benefits for organizations in using unapproved consumer apps:

Faster/easier/available	57%
Able to communicate with anyone	43%
Personal Privacy	31%
Partners use it/require it	28%
Can install it everywhere	23%
Habit/awareness	22%
Policy is unclear/approvals slow	14%
Works better with poor signal	13%
Don't have access to secured app	13%
Approved tool lacks features	10%

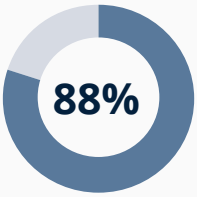
When critical events occur, like outages, cyber-attacks or floods, organizations need more than encrypted channels. **They need unified platforms for coordinated response across teams, agencies, and jurisdictions.**



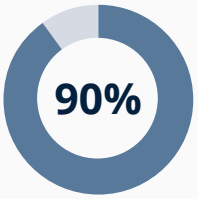
Key Findings

End-to-End Encryption (E2EE) Confusion

Most people trust their messaging apps:



say they're confident in app security for sensitive work



however, don't fully understand what encryption actually protects

Trust in those apps may be high, but understanding is not. This creates a risky gap between perception and reality.

Rising Network Intrusion Concerns

At the network layer, trust is notably lower.

52%

say they are concerned about telecom infrastructure and providers being monitored or disrupted by an adversary

59%

with Singapore the highest

This is not surprising, given recent high-profile reports of telecom infrastructure compromises around the world. However, the gap between app and network trust is a critical and growing distinction when in fact both are vulnerable to adversaries collecting data and metadata at scale.

Device Security Blind Spots

There's broad support for locking devices down:

96%

want secure device mandates

41%

assume encryption already does that

It doesn't, and that gap is leaving devices and organizations exposed.

Certification Shortfall

Security certifications matter:

61%

cite government/industry certifications as critical when choosing a communication tool

38%

still take vendors at their word without independent proof

Assurance is often assumed, not verified.

Key Findings

Sovereignty Paradox

Sovereignty is a priority:

say sovereign control over communications is a priority

however, are using platforms that can't provide it

Control over communications data is demanded but rarely enforced.

A Crisis Confidence Gap

In a crisis or emergency, confidence in communications is high:

93%

believe they're ready to respond

51%

admit they lack a unified communications platform when it matters most

As physical and digital risks continue to escalate, impacting business resilience and personnel safety, organizations are under-prepared.

The Quantum Clock is Ticking

61%

expect quantum computing threats within the next five years

78%

however, haven't implemented defenses

The threat is acknowledged, but preparation is lagging.

Why This Matters Now

Several converging factors demand an urgent response to close a critical perception gap between what organizations believe their security posture provides – and what it actually delivers.

1. Communications: A Target-Rich Environment

Geopolitical tensions have elevated concerns about foreign infrastructure dependency and service availability. The world has increasingly witnessed cyber-intrusions on major global telco-networks. AI-powered deepfakes have made impersonation a viable attack vector. Quantum computing timelines have shortened, and adversaries are already harvesting encrypted data for future decryption. Nation-state actors actively target government and infrastructure communications.

The gap

Organizations assume their communications infrastructure is resilient. In reality, supply chain vulnerabilities, legacy systems, and geopolitical dependencies create exploitable weaknesses that few have fully mapped.

2. New Era of Risk: From Climate to Cyber

Recent years have also stress-tested crisis response capabilities as physical and digital events converge, impacting security, safety and operational continuity. Organizations are discovering that everyday communication tools often fail precisely when coordination demands peak.

The World Economic Forum (2026 Global Risk Report) cites: “Modern economies’ critical infrastructure is becoming increasingly vulnerable to both chronic climate risks and acute extreme weather events, including extreme heat, forest fires, floods and storms. High-impact extreme weather events can cause severe and lasting disruptions to critical infrastructure.”

The question of whether organizations have unified Critical Events Management (CEM) platforms for coordinated response has become pressing – particularly for governments and critical infrastructure coordinating across agencies, jurisdictions, and even borders.

The gap

Most organizations test communications during stable conditions and assume they’ll work in a crisis. When infrastructure fails, supply chains break, or networks are compromised, standard tools become unreliable. Under-prepared institutions pay the steepest price.

3.Year to Quantum (Y2Q) Countdown

The distance between acknowledging quantum timelines and implementing post-quantum cryptography (PQC) resilience creates exposure now, for data with long-term sensitivity. Adversaries are already harvesting encrypted communications today, betting they can decrypt it once quantum computers mature. Any data with long-term sensitivity is an active risk right now. Yet most organizations lack a Cryptographic Bill of Materials (CBOM): a clear inventory of where cryptography is embedded across applications, infrastructure, and supply chains. Without that visibility, migration planning is not possible and supply chain dependencies become unmanaged blind spots. The stakes are significant. The World Economic Forum estimates that cybercrime could cost the global economy US$10.5 trillion annually in the coming years; and quantum-enabled attacks could amplify that risk if encryption standards fail.

What separates organizations making meaningful progress is not speed; it is methodology. A credible PQC migration starts with cryptographic inventory, establishes clear ownership across IT, security, risk, and procurement, and treats supply chain dependencies as a first-order governance question rather than a technical afterthought. The critical questions are not when quantum computers will arrive. They are: how long must specific data remain secure, where does cryptography currently reside across our environment, do our supplies know the same about theirs, and who owns the migration roadmap.

The gap

Most organizations know quantum is coming; but few have answered those questions. Most are tracking to governing body deadlines rather than ahead of them, and deadline-driven migrations under pressure tend to be incomplete. For data with long-term sensitivity, the transition to post-quantum protection cannot wait.

4. The Material Risk: Between Understanding and Reality

Here's where the stakes converge:
Organizations operate with an incomplete understanding of their actual security posture, and this gap creates material, measurable risk.

BELIEF

- Comms tools are crisis-resilient
- Infrastructure withstands hybrid threats
- Crisis coordination is effective

REALITY

- They fail when networks are compromised
- Supply chain vulnerabilities create single points of failure
- Fragmented tools create response delays and information gaps

WHAT ORGANIZATIONS BELIEVE:

- Their communications tools are resilient and will function during crises
- Their data is protected by current encryption standards
- Their infrastructure can withstand hybrid threats (physical + cyber)
- They can coordinate effectively across agencies/borders during emergencies

WHAT MANY DISCOVER TOO LATE:

- Standard comms tools fail when networks are compromised or infrastructure is damaged
- Encrypted data harvested today will be readable post-quantum
- Supply chain vulnerabilities create single points of failure
- Crisis coordination lacks unified platforms, creating response delays and information gaps – impacting operational continuity and resilience
- Third-party dependencies mean security posture depends on vendors they don't fully control

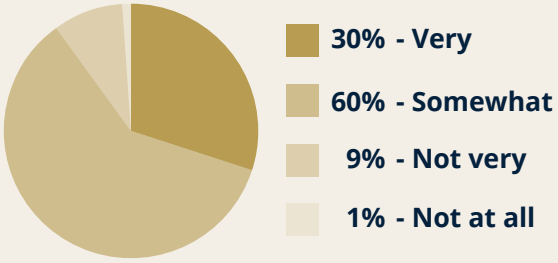
The consequence:

Organizations making procurement, policy, and operational decisions based on incomplete threat understanding may be exponentially more exposed than they realize. When any crisis hits, they discover their "resilient" infrastructure was resilient only under ideal conditions. For government and critical infrastructure sectors facing an uncertain geopolitical climate and escalating risks, this gap is existential.

A 30-minute comms failure during a coordinated attack could lead to cascading infrastructure failures. A breach of encrypted data today could compromise classified information for decades. A supply chain compromise could disable essential services.

> The question is no longer "Can we handle a crisis?" but **"Do we understand how our current tools will fail — and do we have alternatives ready?"**

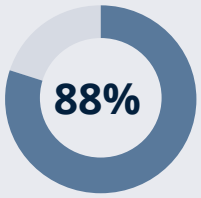
How confident are you that your current approach or processes can manage a major crisis that impacts normal channels/systems of communication?



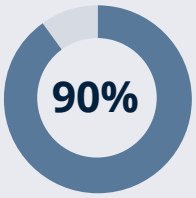
End-to-End Encryption Confusion

End-to-end encryption (E2EE) has become the primary marker of secure communications. When evaluating messaging platforms, organizations look for the E2EE label as assurance that their communications are protected. The term appears in marketing materials, procurement requirements, and security policies as a baseline expectation.

The survey found that 72% of respondents view E2EE as a comprehensive comprehensive security solution. Among the respondents, however, 90% hold misconceptions about what E2EE actually protects. This gap reflects how encryption has been positioned in consumer marketing rather than a failure of technical competence among security professionals.

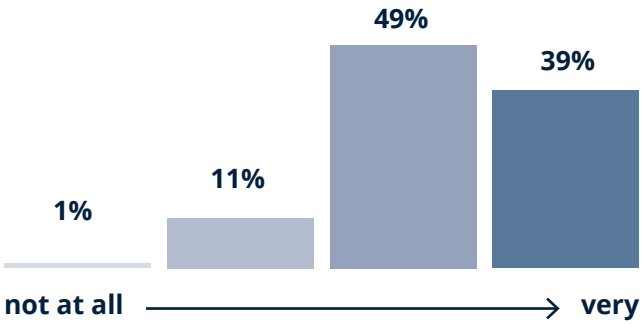


express confidence in consumer messaging app security

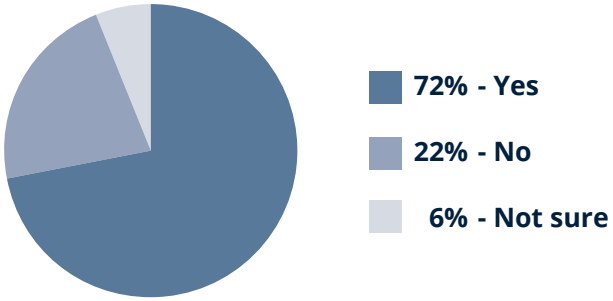


of those relying on E2EE hold misconceptions about what it actually protects

How confident are you that these consumer apps provide sufficient security for sensitive work?



Do you believe end-to-end encryption alone makes a communication system or messaging application secure?



E2EE does not...

- protect data before encryption or after decryption
- hide or protect information about the communication itself (metadata)
- verify or protect the identity of communicating parties
- secure devices that may be compromised

It is one layer of security, not a complete solution.

These misconceptions compound: 32% hold two simultaneous misunderstandings, 18% hold three, and 9% believe all four assumptions above. The result is a significant population of organizations whose security posture rests on incomplete understanding of their primary protection mechanism.

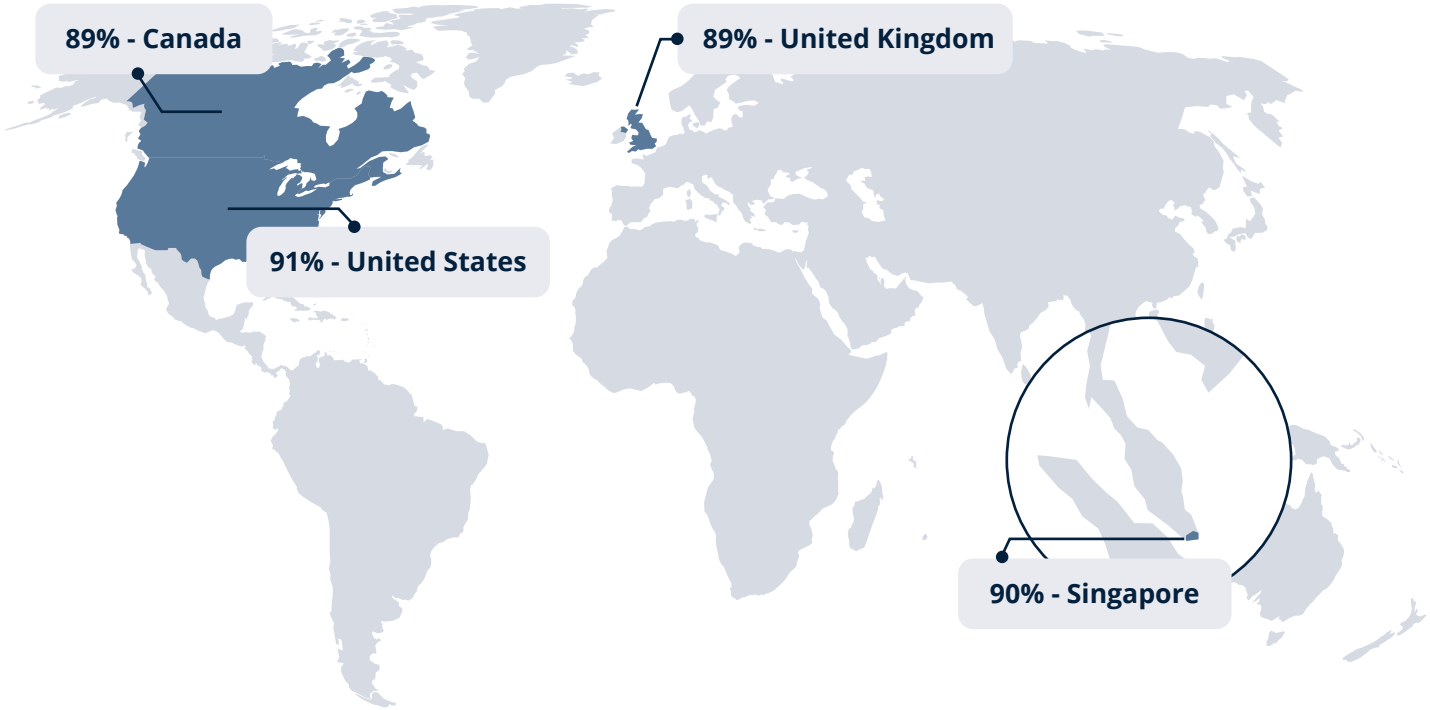
GEOGRAPHIC CONSISTENCY

E2EE misconceptions persist uniformly across all four countries surveyed: Canada (89%), United States (91%), United Kingdom (89%), and Singapore (90%). This tight clustering suggests an industry-wide communication gap rather than regional differences in technical education. The pattern indicates that clearer guidance from the security community could address misconceptions across all markets simultaneously.

When you hear "end-to-end encrypted", what do you assume is protected?

Access to data	57%
Message content	54%
Metadata (IP addresses, locations, contacts)	52%
Identity verification (protection against spoofing)	47%
Communication patterns (who talks to whom, when)	42%
Device integrity (protection if device compromised)	41%

End-to-End Encryption misconceptions across the surveyed countries:

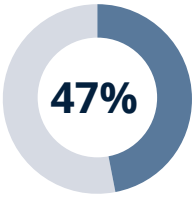


Identity Verification Gap

The identity verification gap is particularly consequential given the current threat landscape. Respondents recognize that impersonation poses serious risk to their communications. Half identify it as a top three concern, and 63% express high concern (level 4 or 5 on a 5-point scale) about deepfake voice, video, or impersonation being used to trick or mislead staff. Yet a large portion (47%) believe their E2EE-labeled tools provide protection against spoofing and impersonation.

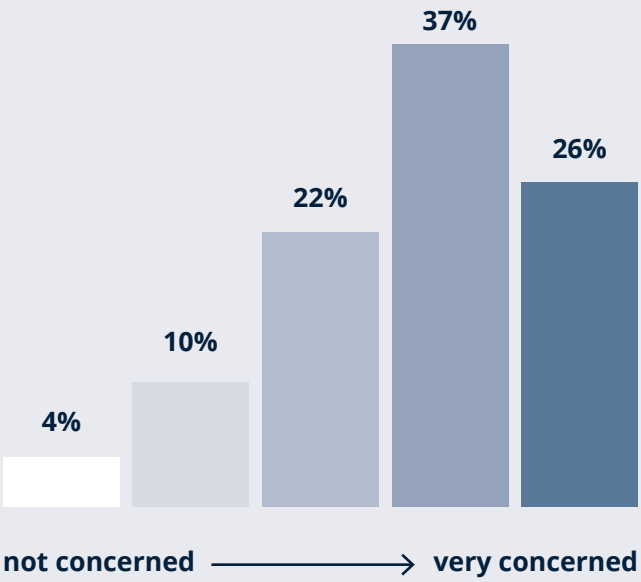
E2EE encrypts message content. It does not verify who is sending or receiving that content. Phone numbers can be spoofed. Accounts can be compromised. Social engineering can add unauthorized participants to group communications. The encrypted channel protects content in transit but does nothing to ensure the people at each end are who they claim to be.

identify impersonation or deepfakes as a top 3 threat to sensitive communications



incorrectly believe E2EE protects against the very threat they fear

How concerned are you about deepfake voice, video or impersonation being used to trick or mislead staff?



What do you believe are the greatest risks to your mission-critical and sensitive communications?

Leakage of personal metadata	55%
Device compromise	54%
User impersonation or deepfakes	50%
Messages being compromised by an adversary	37%
Telecom or provider compromise	29%

Metadata Exposure Gap

Adding to exposure concerns at the network layer, more than half of respondents (52%) reported being concerned or very concerned about the risk of telecom infrastructure and providers being monitored or disrupted by an adversary. Concern was highest in Singapore (59%), followed by Canada at 54%, the UK at 50%, and the US at 49%.

While E2EE encrypts the content of messages, metadata remains visible to platform operators and potentially to adversaries who can access platform infrastructure or intercept traffic. Metadata includes who communicated with whom, when communications occurred, how frequently parties communicate, the duration of communications, device identifiers, IP addresses, and location data.

For intelligence purposes, metadata can be as valuable as content. Communication patterns reveal organizational structures, identify key personnel, expose relationships between entities, and signal operational changes. Location metadata tracks physical movements. Timing patterns indicate working hours, travel schedules, and response to events. An adversary with access to metadata can map an organization's structure, identify high-value targets, and monitor activities without reading a single message.

In sensitive environments, who attended a meeting may matter as much as what was discussed. E2EE protects the discussion but not the attendance record.

52%

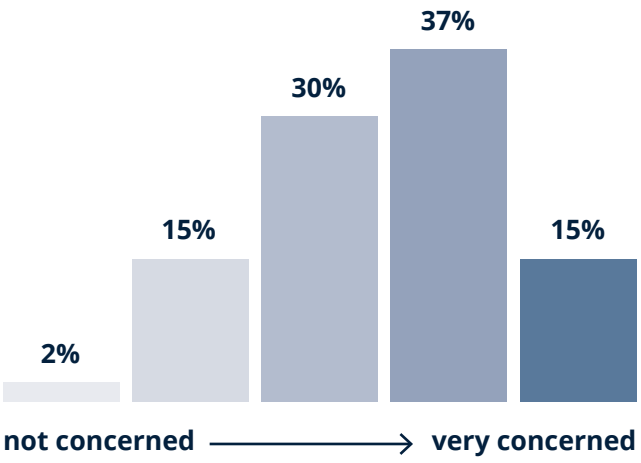
of respondents incorrectly believe E2EE protects metadata.

This misconception has significant operational implications.

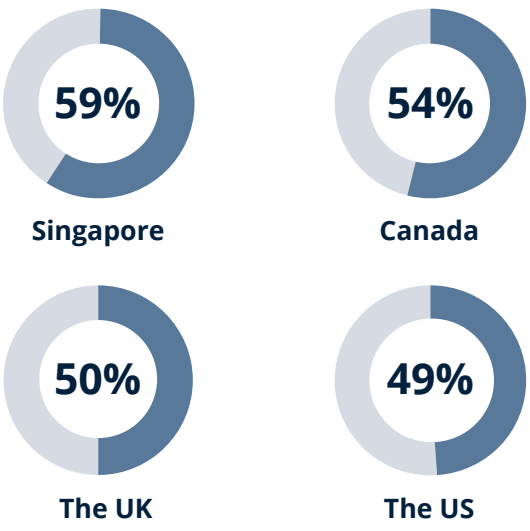
Metadata includes...

- Who communicated with whom
- When communications occurred
- How frequently parties communicate
- The duration of communications
- Device identifiers
- IP addresses
- Location data

How concerned are you that telecom infrastructure/providers could be monitored or disrupted by an adversary?



Concern by country



Device Blindspot

The device blind spot reveals a gap between what organizations want and what they believe they have. Nearly all respondents (96%) support requiring verified, secure devices for sensitive communications. This near-universal support indicates that organizations understand device security matters.

Yet among respondents that view E2EE as comprehensive security, 41% believe it protects communications even if devices are compromised, stolen, or infected with malware. This creates a false sense of security. Respondents believe they need device protection (hence support for mandates) while simultaneously believing their current encryption provides it (hence not implementing separate controls).

96%

support mandating verified, secure devices for sensitive communications

41%

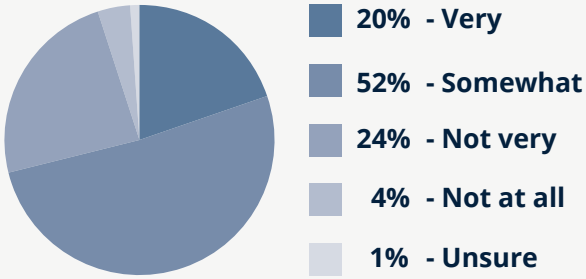
believe encryption already protects compromised devices. It doesn't.

WHAT E2EE CANNOT PREVENT

- Malware reading messages before encryption or after decryption
- Keystroke loggers capturing content as it is typed
- Screen capture tools recording messages as they are displayed
- Stolen devices exposing stored message history
- Rooted or jailbroken devices bypassing application security
- Unauthorized users added to group communications without verification
- Clipboard attacks capturing copied message content

These attack vectors are not theoretical. Nation-state adversaries deploy sophisticated mobile malware. Criminal organizations use commodity spyware. Lost or stolen devices create exposure even without sophisticated attacks. Each of these scenarios bypasses E2EE entirely because the compromise occurs outside the encrypted channel.

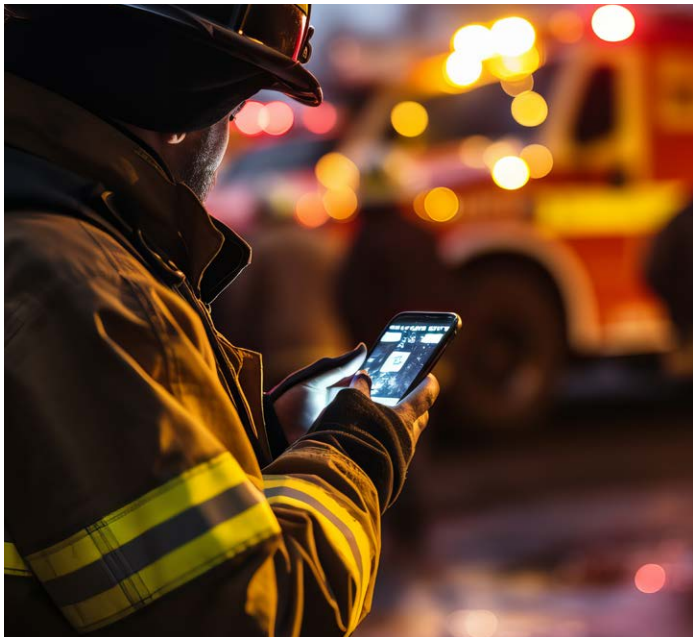
Confidence in Device Security Despite E2EE Limitations



72%

express confidence (very or somewhat) in their company's device security

This confidence persists despite the misconceptions about E2EE's protection scope. The gap between stated support for device security mandates and belief that current tools already provide device protection suggests organizations may not be implementing the additional controls their own risk assessments would indicate.



Device security requires controls distinct from transit encryption: malware detection and prevention, cryptographic containerization that isolates sensitive applications, encryption at rest for stored data, device attestation that verifies hardware integrity, and mobile device management that enforces security policies. These are not features E2EE provides.

Key Insight: Respondents recognize device security matters

96%

support mandates

41%

however, believe encryption already provides this

The device represents a critical security boundary that E2EE does not address. Transit security and endpoint security are distinct domains requiring different controls, and both are necessary for secure communications.

Certification Shortfall

The certification shortfall helps explain how the misconceptions documented above persist. Respondents know independent verification matters. They cite government certifications, third-party assessments, and recognized standards as important factors in selecting communication tools. Yet a substantial minority still accept vendor claims without independent validation.

When vendors market E2EE as comprehensive security, organizations relying on marketing claims rather than independent assessment inherit those positioning choices. The misconceptions about E2EE protection scope documented in this research become predictable outcomes when 38% of organizations rely on vendor self-attestation as part of their evaluation process.

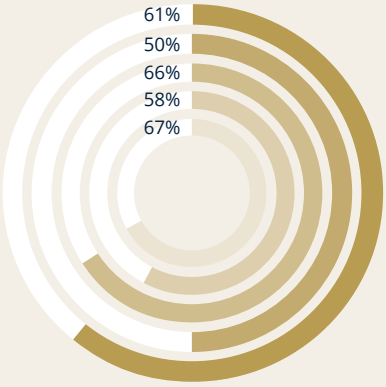
61%

cite government/industry certifications as critical for selecting security tools

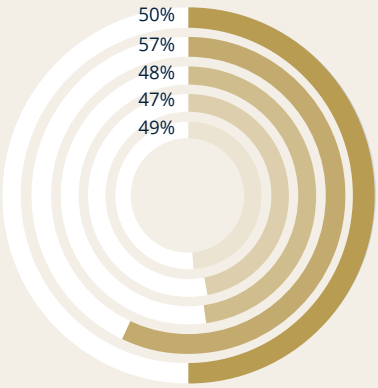
38%

still rely on vendor marketing claims or self-attestations

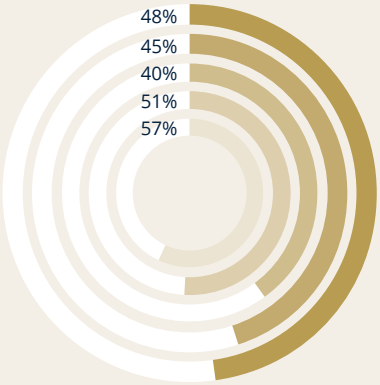
Security Frameworks that matter most when choosing a communication tool:



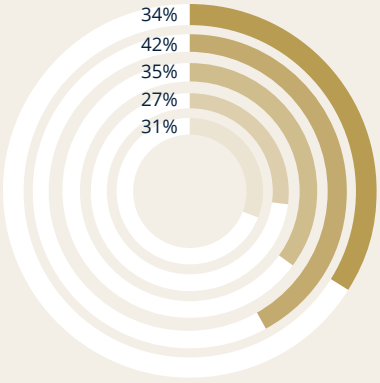
Government/Industry certifications



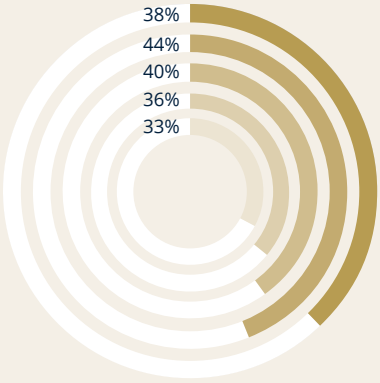
Independent third-party assessments



National directives/ approvals

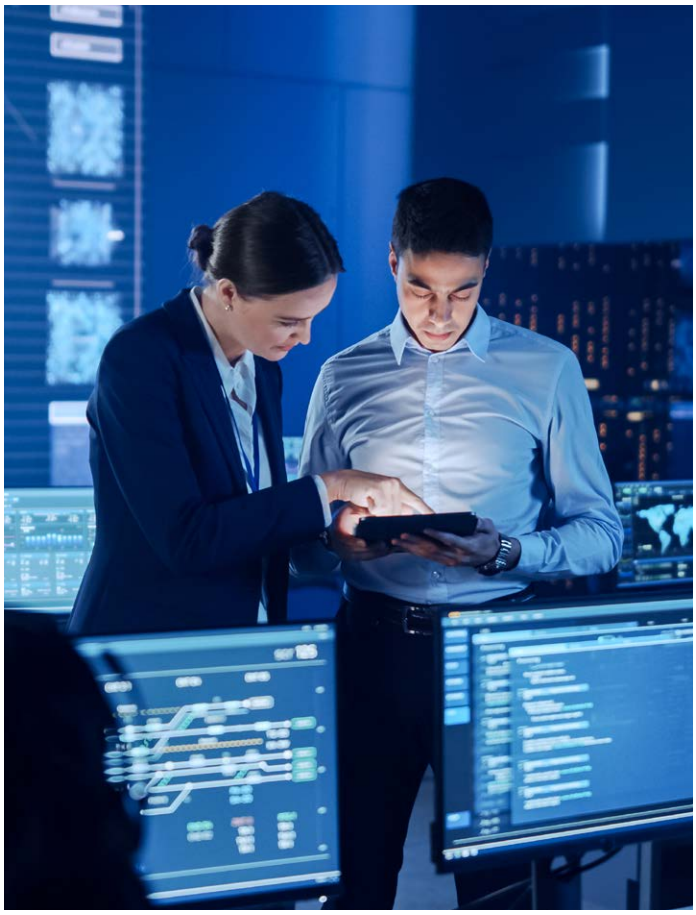


Recognized crypto modules



Vendor marketing/ self-attestations

> The US shows the highest reliance on vendor self-attestations and the lowest reliance on government certifications. **A concerning combination given the E2EE misconceptions documented above.**



Geographic variation in verification practices is notable. US respondents show the highest reliance on vendor marketing claims (44%) and the lowest reliance on government certifications (50%). Singapore shows the opposite pattern: lowest reliance on vendor claims (33%) and highest reliance on government certifications (67%). UK and Canada fall between these poles.

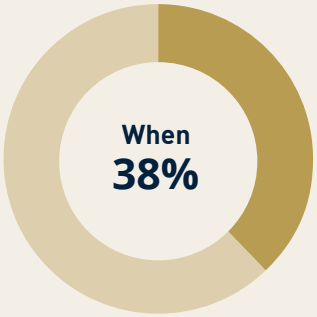
These patterns suggest different regulatory environments and procurement cultures shape how respondents evaluate security tools. In markets where vendor claims carry more weight, the misconceptions created by marketing positioning can propagate more readily.

A transition in progress

These findings suggest the industry may be moving toward requiring government or independent proof of security capability. Respondents citing certifications and independent assessments outnumber those relying on vendor claims. But the transition is incomplete. A strong argument exists for all organizations to complete this transition as quickly as possible, replacing vendor self-attestations with verified, independent validation of security capabilities.

> These findings suggest the industry is moving toward **requiring government or independent proof of security capability.**

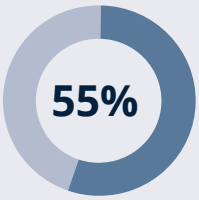
Key Insight: Reliance on vendor claims creates predictable outcomes



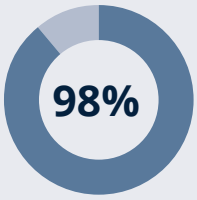
of respondents accept marketing messaging without independent verification...

...the misconceptions documented throughout this research follow naturally. Independent verification through government certification and third-party assessment provides a more reliable baseline for security procurement decisions.

Sovereignty Paradox



prioritize full sovereign control over communication systems



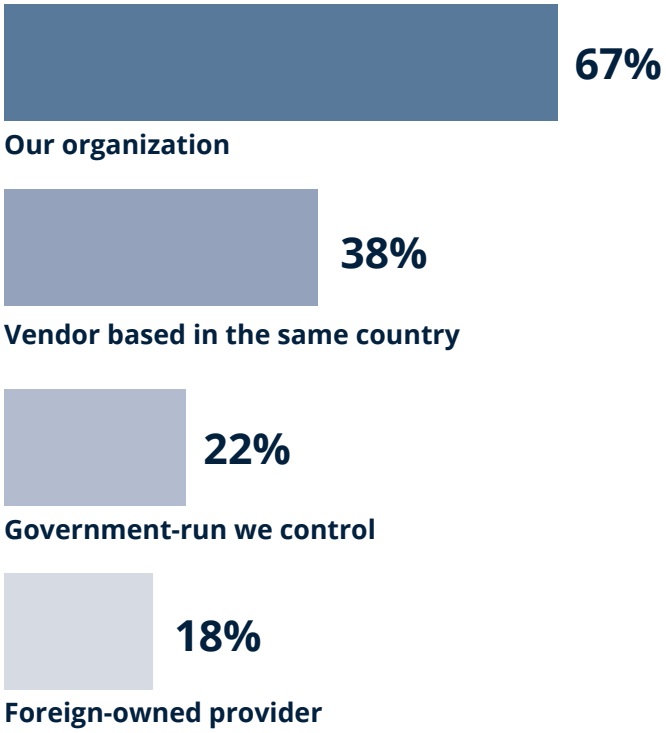
of those same organizations use consumer platforms that operate on foreign infrastructure

More than half of respondents (55%) identify full sovereign control as a priority for their communication systems. These organizations require domestic data residency, infrastructure independence, and freedom from foreign legal jurisdiction. Sovereignty requirements often stem from regulatory mandates, national security policies, or organizational risk assessments that identify foreign infrastructure dependency as unacceptable.

Yet among respondents with sovereignty requirements, 98% acknowledge using consumer messaging platforms. WhatsApp, Teams, Signal, and similar applications operate on infrastructure located outside most users' domestic jurisdictions. Their servers, data centers, and operational control sit in foreign countries, subject to foreign laws.

> The same design that makes these platforms easy to deploy and use across borders makes them **structurally incompatible with sovereignty requirements.**

Who currently controls organization's core communication systems:



This is not a compliance gap that policy updates can close. It is an architectural impossibility. Consumer messaging platforms are built on centralized, globally distributed infrastructure. Their convenience and ubiquity come precisely because they do not maintain separate sovereign instances for each country. The same design that makes these platforms easy to deploy and use across borders makes them structurally incompatible with sovereignty requirements.

When balancing the benefit of open communication and the security of data sovereignty which would you prioritize?

Full sovereign control	**55%**
Ease of global connectivity	**36%**

The Kill Switch Risk

Sovereignty is not only about data security. It is about service availability. Foreign-hosted platforms can be turned off, throttled, or denied at the discretion of the host country's government. During geopolitical tensions, trade disputes, or international incidents, critical communication infrastructure could be disabled regardless of encryption strength. Organizations relying on foreign platforms have no recourse if service is suspended. No domestic legal framework protects access to infrastructure controlled abroad. Cryptographic security becomes irrelevant when the service itself is unavailable.

Key Insight: The question is not whether consumer platforms encrypt communications.

The question is whether they can be sovereign and whether they will be available when needed.

Foreign infrastructure means foreign control: over data access, over encryption keys, and over whether the service operates at all. Sovereignty and consumer platform convenience are structurally incompatible.

The risk extends beyond data access. Foreign-hosted services can be suspended, restricted, or terminated based on the host country's foreign policy decisions, sanctions regimes, or geopolitical disputes. Organizations have no legal recourse in domestic courts when infrastructure is controlled abroad. During a crisis, precisely when secure communication matters most, the service itself could become unavailable.

Organizations face competing pressures. Sovereignty policies demand domestic infrastructure control. Operational needs drive adoption of widely available consumer platforms. Staff already use these tools personally and expect to use them professionally. The convenience and interoperability of consumer apps creates structural tension with sovereignty requirements that those apps cannot satisfy.

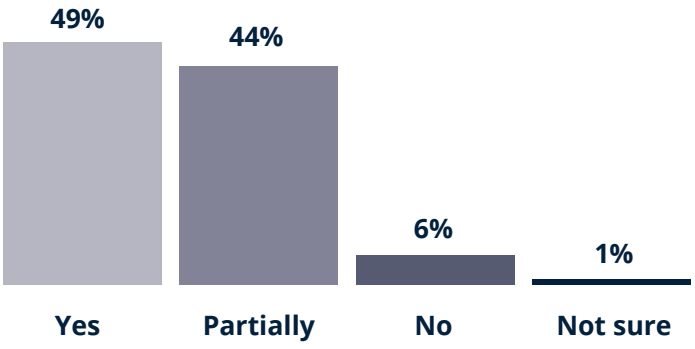
Crisis Confidence Gap

Crisis communication presents unique challenges. Normal communication tools may be inadequate when infrastructure is compromised, when coordination must span multiple agencies and jurisdictions, when staff safety must be tracked in real time, and when decisions must be made under extreme time pressure with incomplete information.

The survey found that 90% of respondents express confidence in their organization's ability to manage major crises. This confidence spans specific capabilities: detecting and assessing threats, sending mass alerts, notifying staff and tracking their safety, mobilizing resources, coordinating across agencies and jurisdictions, maintaining operations under stress, and tracking outcomes in near real time.

Yet only 49% have unified Critical Events Management (CEM) platforms that provide these capabilities in an integrated system.

During a crisis or critical event, does your organization have a CEM system or a single, governed view to monitor alerts, staff/people status, chats, calls, situational status to coordinate across teams?



MOST USED COMMUNICATION TOOLS DURING CRISIS:

Small group chats	56%
Email threads	53%
1-to-1 chats	41%
Manual bridges or conference calls	31%
Shared documents/spreadsheets	30%
Phone trees	19%
Radio/LMR channels	7%

Organizations without unified CEM platforms coordinate using familiar everyday tools. They create group chats to share updates, send email threads for directives, use phone trees to reach personnel, track status in shared spreadsheets, and set up conference bridges for coordination calls. These tools are familiar and available, but familiarity is not capability.

Crisis Confidence Gap

90%

are confident in their organization's crisis response should political pressure or sanctions arise

51%

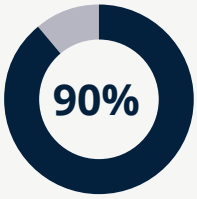
lack unified crisis management platforms. Instead they rely on email, group chats, and spreadsheets.

The gap between confidence and capability becomes critical during actual emergencies. Everyday tools lack the unified situational awareness that crisis response demands. There is no single operational view of staff status. Alert coordination happens across multiple disconnected channels. Action tracking requires manual aggregation. Cross-jurisdiction coordination depends on ad hoc relationships rather than established protocols and systems.

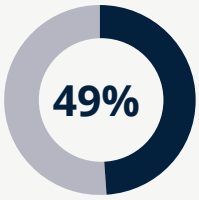
Crisis response often requires coordination across multiple agencies and jurisdictions, each with their own communication systems and protocols. Without federated CEM architectures, each organization operates in isolation. Local emergency services cannot coordinate seamlessly with state authorities. State systems cannot integrate with federal response. Cross-border incidents lack unified command structures. The organizations involved may each believe they are prepared while the seams between them remain untested.

> The gap between confidence and capability may only become visible during an actual crisis, **when it is too late to address.**

Key Insight:



confidence measured against...



actual capability represents a dangerous gap

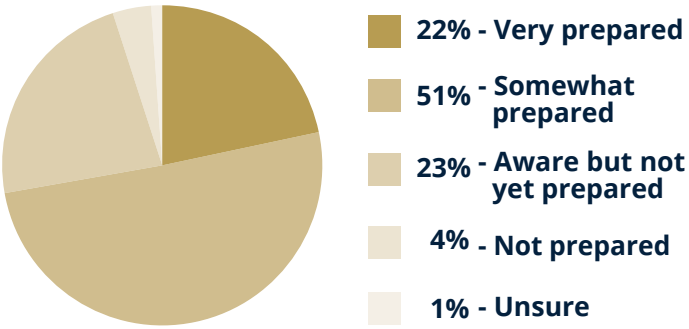
When infrastructure fails and time pressure is acute, email threads and group chats cannot provide the unified command and control that crisis response demands. The gap between confidence and capability may only become visible during an actual crisis, when it is too late to address.

Quantum Countdown

Quantum computing represents a different kind of security challenge than the gaps documented above. The other findings describe current mismatches between perception and capability. The quantum gap describes a future threat that creates present-day vulnerability.

Current encryption relies on mathematical problems that classical computers cannot solve in practical time. Breaking modern encryption through brute force would take longer than the age of the universe with current technology. Quantum computers operate differently, using quantum mechanical phenomena to solve certain problems exponentially faster than classical computers. The specific problems quantum computers accelerate include those underlying widely deployed encryption algorithms.

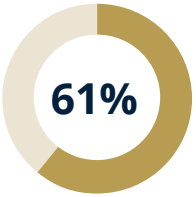
Post-Quantum Cryptography Implementation Status



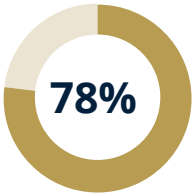
Why Quantum Computing matters for encryption:

Current public-key cryptography relies on the difficulty of factoring large numbers and computing discrete logarithms. Classical computers cannot solve these problems efficiently. Quantum computers running Shor's algorithm can. Post-quantum cryptography (PQC) uses different mathematical foundations that resist both classical and quantum attacks.

Transitioning to PQC requires updating cryptographic implementations across all systems; it is not a single product decision. It is a multi-year program that touches certificates, protocols, hardware, software, vendors, budgets, and procurement cycles simultaneously. Organizations that build for crypto agility, architecting infrastructure to substitute algorithms without rebuilding from scratch, will be better positioned for this transition and for future cryptographic standard changes.



assess that quantum computing will threaten current encryption within five years



have not yet implemented post-quantum cryptography

The Harvest Window is already open:

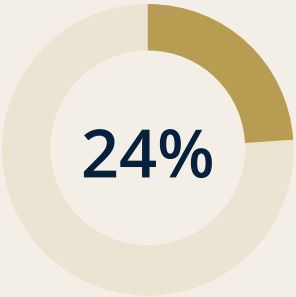
Unlike other security gaps, quantum creates vulnerability that extends backward in time. Adversaries harvesting encrypted communications today do not need to wait for organizations to implement post-quantum cryptography. They are already collecting data that future quantum capabilities will unlock. Data with long-term sensitivity is at risk today regardless of when quantum computers become capable.

Main reasons for organizations to not be prepared to transition to PQC:

- **Lack of internal expertise/resources**
- **Not seen as immediate threat**
- **Waiting for formal government guidance**
- **Competing mission priorities/limited budget**

61% of respondents assess that quantum computing will pose practical threats within five years. The majority have strategies defined (51%) or are in early planning (23%); only 22% have reached active implementation.

That gap reflects the genuine complexity of PQC migration rather than indifference to the threat. The technical migration is solvable. The harder problem is organizational: building a cryptographic asset inventory, aligning stakeholders, and securing multi-year budget commitments before pressure becomes acute. The organizations navigating this well treat PQC migration as a governance program first and a technology project second.



express high concern about "harvest now, decrypt later" attacks

Yet among this concerned group, most still have not completed implementation.

The "harvest now, decrypt later" scenario is not theoretical. Nation-state adversaries are known to collect and store encrypted traffic. The stored data costs little to keep. When quantum decryption becomes available, previously collected intercepts become readable. Communications that seemed secure when transmitted may be compromised years or decades later.

The gap between perceived timeline (61% expect five-year threats) and implementation status (78% not yet implemented) reflects real procurement and technical constraints. But the harvest window does not wait for procurement cycles. For organizations holding long-term sensitive data, the governing body deadlines of 2030 are not the only clock running. The more relevant question is how long the data needs to stay protected, and when it first became a collection target.

Key Insight

Most organizations know quantum computing is coming and have begun to plan. Data encrypted with vulnerable algorithms today remains exposed regardless of future implementation.

The organizations that meet the 2030 deadlines will be the ones that started in 2025 and 2026, treating PQC migration as a governance priority rather than a future project.

What This Means

The six gaps documented in this research share a common pattern: organizations believe one thing while doing another.

They recognize threats but trust tools that do not address them. They require capabilities their platforms cannot provide. They express confidence that exceeds their actual preparedness.

The root cause is not technical failure. These security technologies work as designed. E2EE does protect message content in transit. Device security controls do protect endpoints when implemented. Independent verification does provide reliable security assessment. Sovereign infrastructure does deliver domestic control. Unified CEM platforms do enable coordinated crisis response. Post-quantum cryptography does resist quantum attacks.

The failure is in translation: between what security tools do and what organizations believe they do, between policy requirements and infrastructure architecture, between confidence and capability. This translation failure has been enabled by marketing that emphasizes strengths while obscuring limitations, by procurement processes that accept vendor claims without independent verification, and by the natural human tendency to believe that visible security measures provide comprehensive protection.

Perhaps the most telling finding: 86% of respondents say they would be “somewhat” or “very surprised” if their organization’s sensitive communications were compromised tomorrow. Despite the misconceptions documented throughout this research, despite the policy-practice gaps, despite the architectural incompatibilities, organizations do not recognize their own exposure. The confidence is genuine. Whether it is justified is the question this research raises.

> **Closing these gaps starts with recognizing them** and demanding answers that go beyond marketing claims to independent, verifiable proof of capability.

Three Questions Every Security Leader Should Ask:

Beyond the Label

What specific threats does our encryption address, and which require separate controls? Map E2EE protection boundaries against actual threat models. Identify where metadata protection, identity verification, and device security require distinct solutions. Do not assume that “encrypted” means “secure.”

Architecture vs. Policy

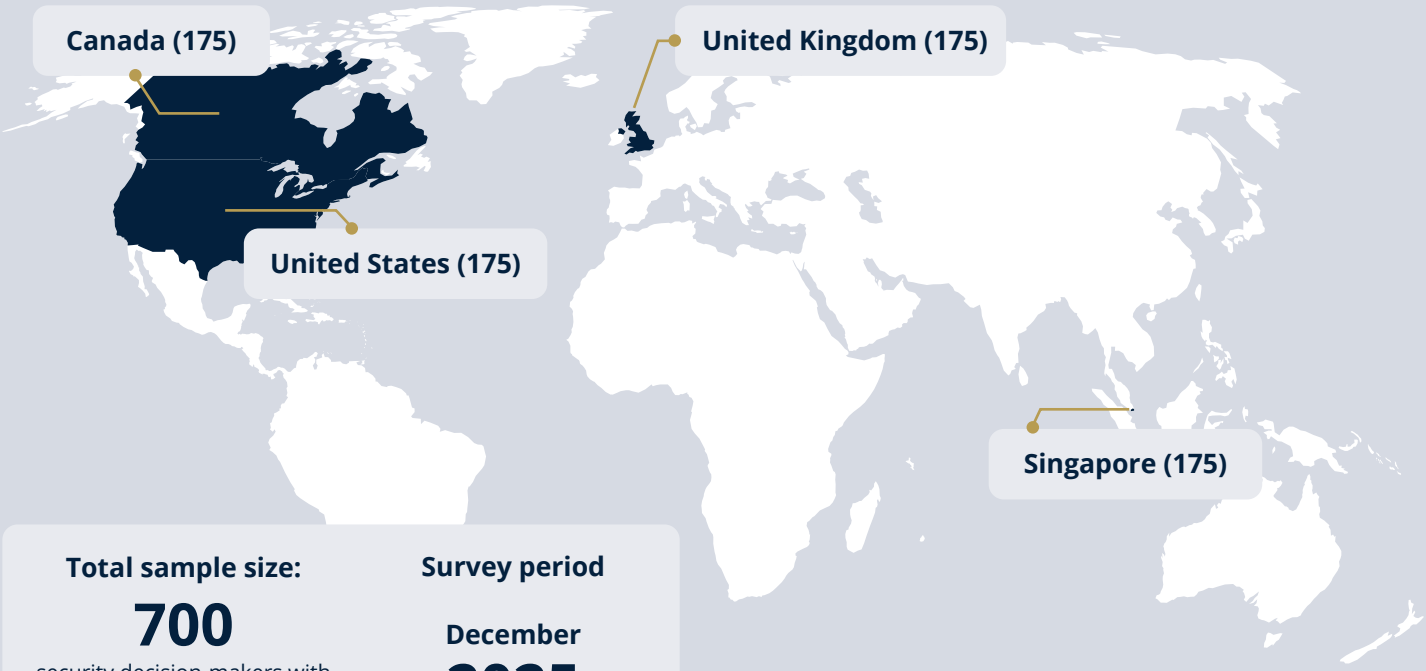
Do our platform choices structurally support our sovereignty and compliance requirements? If policy mandates domestic control, audit whether infrastructure architecture can deliver it. Otherwise we may have requirements our platforms cannot fulfill, creating compliance exposure and operational risk.

Confidence Audit

Is our crisis preparedness measured against demonstrated capabilities or assumed ones? Test unified response across teams and jurisdictions. Verify that confidence reflects actual capability, not familiarity with everyday tools that may fail under crisis conditions.

Methodology

RESPONDENTS BY REGION:



Total sample size:

700

security decision-makers with visibility into organizational communication practices

Survey period

December 2025

ABOUT THIS RESEARCH

This report is based on research conducted on behalf of BlackBerry Secure Communications by OnePoll in December 2025. We surveyed 700 security decision-makers in North America, the UK and Singapore. The research examined how government and critical infrastructure organizations perceive and implement secure communications. Questions covered six domains: encryption understanding, device security, infrastructure sovereignty, crisis management capabilities, quantum preparedness, and security procurement criteria. Findings reflect self-reported perceptions and practices among security decision-makers. The research was designed to identify gaps between security confidence and security capability, with particular attention to areas where organizational assumptions may not match technical reality.

Glossary

Consumer Messaging Apps

Platforms like WhatsApp, Telegram, Signal, and standard SMS were tools designed for personal communication and have been informally adopted by organizations for workplace use. The foundation for this description is:

- They have no administrative oversight or control
- Messages can't be formally tracked or audited
- There's no way to verify who has or hasn't seen a message
- They weren't built to compliance or enterprise security standards
- Staff may not have them installed, or may have notifications turned off

What is E2EE?

End-to-end encryption protects message content during transmission. Data is encrypted on the sender's device and decrypted only on the recipient's device, preventing interception during transit. This protection is valuable but limited in scope.

The Deepfake Dimension

AI-generated deepfakes can now impersonate voices and video in real-time. An attacker who gains access to a communication channel (or creates a spoofed one) can pose as a trusted colleague with synthetic voice or video that passes human verification

True identity verification requires cryptographic authentication:

Device attestation that proves hardware identity, key validation that cannot be forged, and continuous authentication that persists beyond initial login. Consumer platforms typically verify identity through phone numbers or email, offering no protection against sophisticated impersonation.

Where E2EE operates

End-to-end encryption creates a protected tunnel for data in transit between two endpoints. The encryption happens on the sending device and decryption happens on the receiving device. This means E2EE has no visibility into or control over what happens on the devices themselves. If a device is compromised, attackers can access messages before they are encrypted or after they are decrypted, completely bypassing the protection E2EE provides.

What Sovereignty requires

Sovereignty over communications infrastructure means domestic control of the physical and operational elements that handle sensitive data. This includes servers located within national borders, data centers operated by domestic entities, encryption key management under domestic control, operational staff subject to domestic jurisdiction, and freedom from foreign legal compulsion mechanisms. Sovereignty determines who can access data under court order, who controls encryption keys, who can be ordered to provide access, and who can be compelled to install backdoors.

ABOUT BLACKBERRY SECURE COMMUNICATIONS

BlackBerry® Secure Communications delivers purpose-built solutions for secure communication, collaboration, and robust crisis management. Engineered to protect high-stakes organizations from evolving communications threats, BlackBerry Secure Communications provides operational continuity for critical functions.

Learn more at: BlackBerry.com/SecureCommunications

BlackBerry | Secure Communications