• STANDING GUARD •




# CONSEQUENCE

The Report for Organizations That Must Secure The World's Most Sensitive Communications

SENTRIQS

## Methodology

In September 2026, a U.S.-based market research firm administered an online survey to **500** respondents across **five industries** in the United States: **state/federal government**, **defense**, **financial services**, **healthcare** and **pharmaceuticals**, and **energy/utilities**. Respondents include full-time practitioners responsible for securing sensitive communications, such as information technology, cybersecurity, logistics, and operations personnel, as well as executives and leaders who hold confidential and high-consequence conversations.




# CONTENTS


03 Security on Paper vs. Security in Practice

08 The Boundary Is the Weak Point

09 Secure Comms Require Control and Governance

09 AI and Quantum Add New Complications

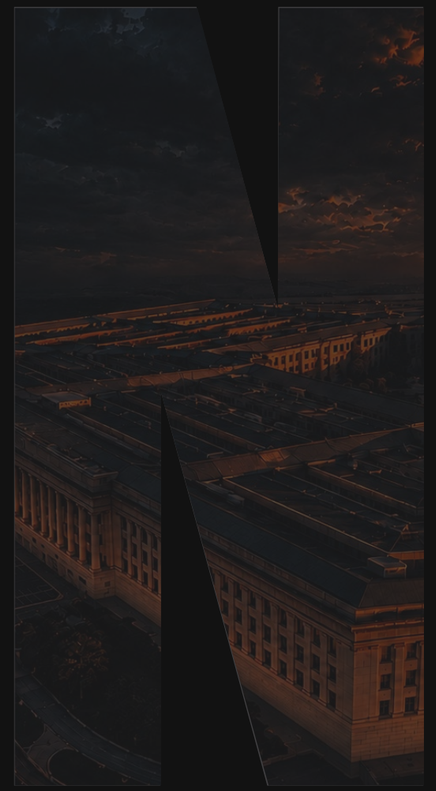
12 The Human Cost Of Accountability

13 Security Is a Shared Responsibility

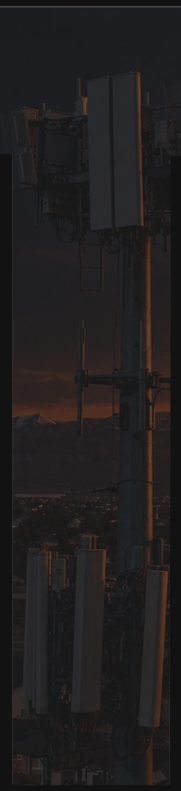
13 From Security Intent To Security by Design

14 A More Secure, Compliant Communications Future

# DISCONNECT







## EXECUTIVE SUMMARY

From hospitals to police departments, banks to government agencies, organizations grapple with security challenges ranging from physical to cyber. These organizations often share sensitive, confidential information that can't fall into the wrong hands. The consequences are materially damaging, or worse, life-threatening.

Despite these consequences, many of the world's most regulated organizations still communicate across teams and partners using tools designed for ordinary business. Those tools have critical gaps in security, access, interoperability, and compliance. The gaps carry serious consequences, from upending an important business deal to undermining military operations that risk lives.

Sometimes, organizations believe they have the right tools but lack a cohesive understanding of what actually constitutes a secure tool, or they don't consistently enforce policies. Security also falters when employees fail to consistently practice the secure behavior an organization expects.

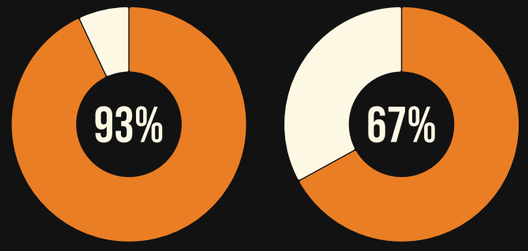
This report magnifies the state of secure communications. Analysis reveals notable themes, from expectations and demands to behavior and readiness.

Significant disconnects exist between security-in-principle and security-in-practice. This report dives into what drives these disconnects, the impact of those disconnects, and how organizations can improve their security posture as the threat landscape becomes more complex with the advance of AI and quantum computing.

# Security on Paper vs. Security in Practice

The dichotomy between principle and practice stems from a significant gap between perceptions of security and reality.

The bulk (**96%**) of the study's respondents say their sensitive communications are secure. In the finance sector, **100%** of respondents believe their sensitive communications are secure. That sentiment is slightly lower for military and defense (**94%**), with government at **96%** and both healthcare and energy/utilities at **95%**, but all industries clearly feel that sensitive, confidential communications are protected.




*Have the right tools for sensitive communications*

*Their organization is prepared to secure sensitive communications*

However, when it comes to the importance of securing sensitive communications, almost one in three (**32%**) respondents say it's not a high priority. This suggests misunderstandings or misperceptions about the risks that sensitive communications face or the potential for them to go awry.

In addition, confidence does not equate to proper behavior. Almost a quarter (**23%**) of study respondents say their colleagues do not always follow security policies. Having the right tools in place does not mean that individuals will use them correctly, or at all.

Closing the gap between security in principle and practice requires addressing the age-old tradeoff between ease of use and security. Of respondents who personally admit to using non-compliant tools, the general consensus (**84%**) is that existing alternatives are more user-friendly than sanctioned tools.

In fact, one in five respondents admit they conduct sensitive, high-consequence conversations with communications tools that do not comply with security policies. Surprisingly, the defense/military sector leads all industries in the study, with more than one in four

**OUR SENSITIVE COMMUNICATIONS ARE SECURE...**

**100%**
**Finance**

**96%**
**Government**

**95%**
**Healthcare & Energy**

**94%**
**Defense**

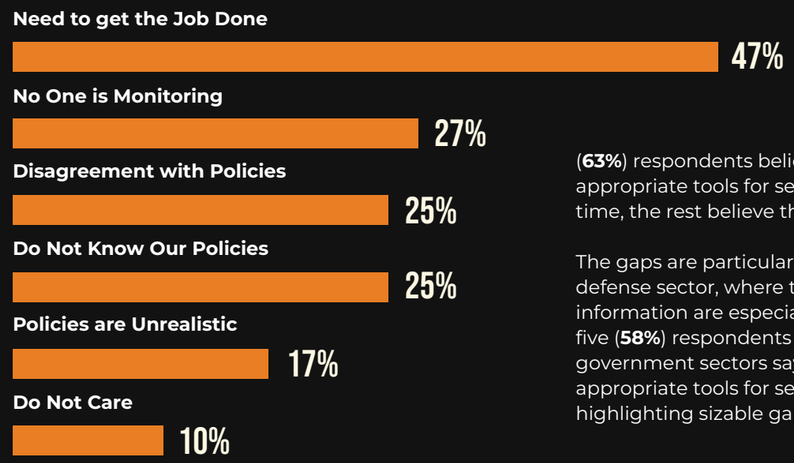
(**28%**) respondents admitting this behavior. Energy follows closely at **26%**.

There's a gap between what employees say and what employers believe. The challenge is not simply having secure communications. Employees also must know how and why to use them, and they must do so consistently. While almost two out of three



## Why has your department broken its security policies?

*(Select all that apply)*

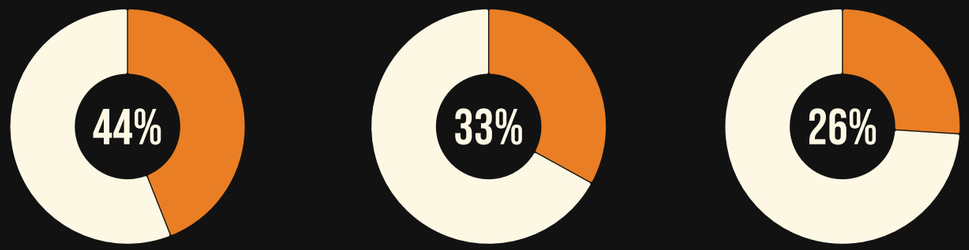



(**63%**) respondents believe their employees use the appropriate tools for sensitive communications all the time, the rest believe they are less diligent.

The gaps are particularly striking in the military/defense sector, where the stakes of protecting sensitive information are especially high. Less than three out of five (**58%**) respondents in both the military/defense and government sectors say their employees always use appropriate tools for sensitive/confidential information, highlighting sizable gaps in diligence.

## Why do your employees not always use the appropriate tools to protect your organization's communications containing confidential, classified, or other highly sensitive information?

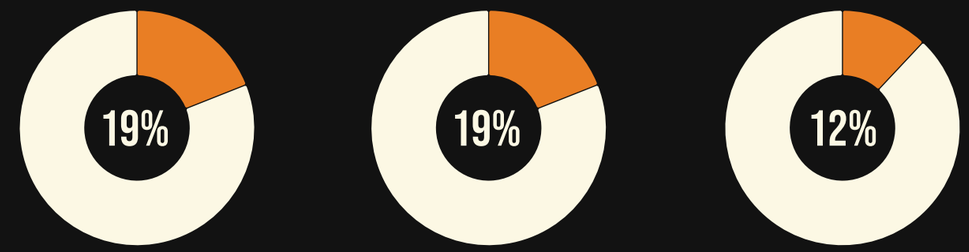
*(Select up to two)*




*Inconvenient*

*More Comfortable with Other Tools*

*Do Not Prioritize Security*




*Too Slow*

*Too Complicated*

*Do Not Believe the Tools Are More Secure*

# MILITARY AND DEFENSE (28%) IS SIGNIFICANTLY MORE LIKELY THAN GOVERNMENT AND HEALTHCARE (15% EACH) TO HAVE USED A NON-COMPLIANT TOOL.

This underscores a broader organizational challenge: Secure communications cannot depend on individual judgment alone. Organizations need clear, consistent expectations and leadership that make secure practices the norm, and this is obvious yet elusive.

Even if the high percentage of perceived secure communications aligns with policy-driven behavior, respondents are overconfident in the security capabilities of commonly used tools. Respondents believe their sensitive communications are secure, but there's a discrepancy in the channels they use for this purpose.

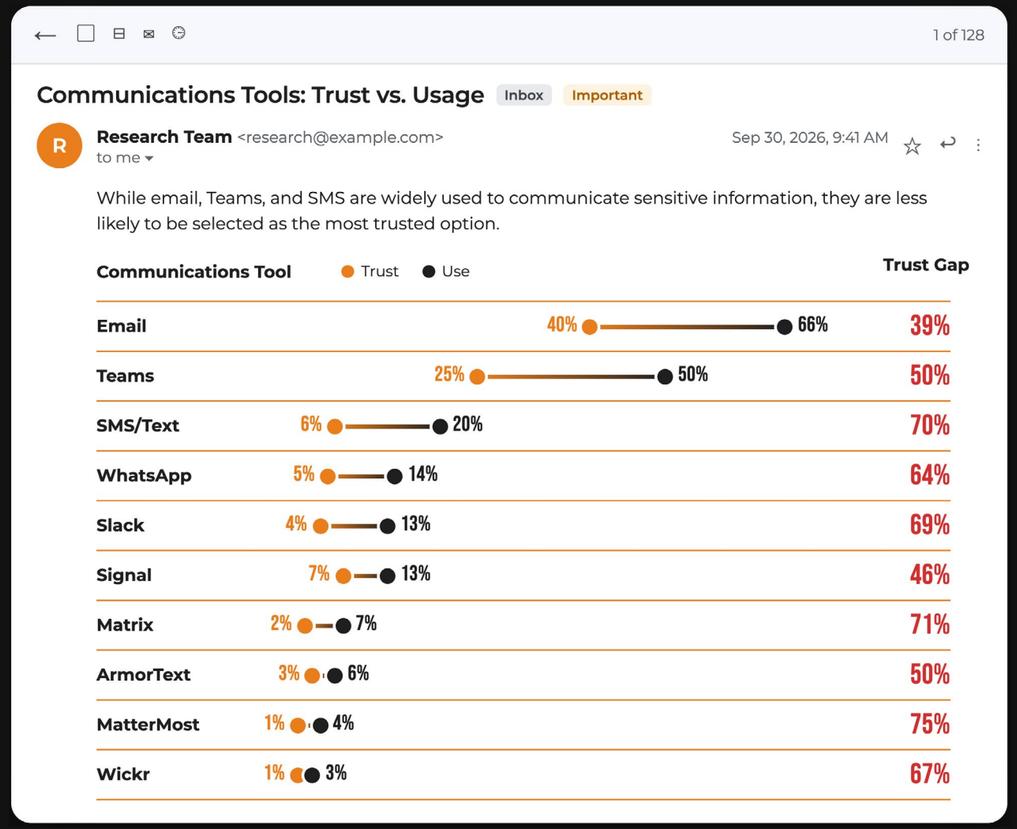
Across all sectors, email (**66%**) is the most common channel for communicating such information. Microsoft Teams is second (**50%**), cited by half of the study's respondents. Others include SMS/text, WhatsApp, Slack, and Signal. Notably, Signal is used mostly in the military/defense sector (**25%**).

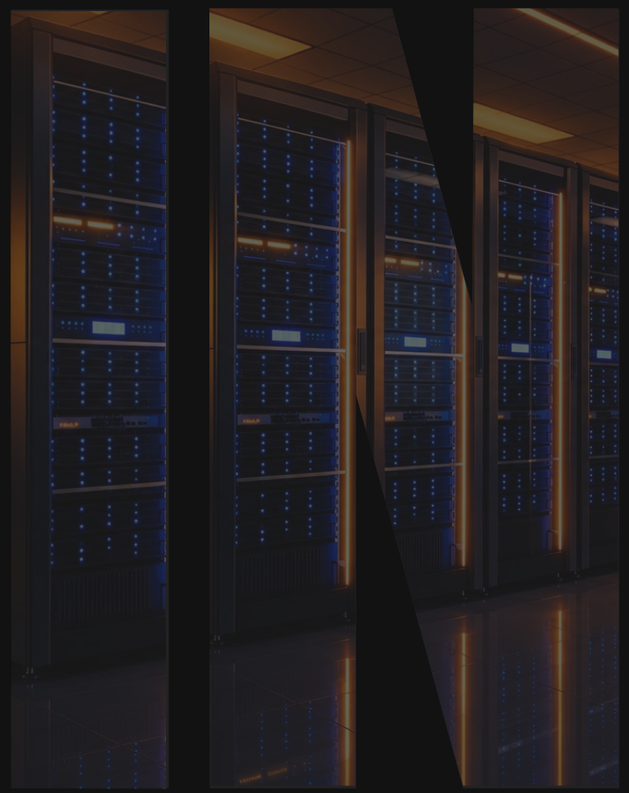
An interesting contradiction emerges: Although respondents use email and Slack for sensitive communications, that doesn't mean they trust them. While two-thirds of respondents say they use email for sensitive communications – be it organizational transitions, military operations, mergers and acquisitions, etc. – only **40%** trust it. Just a quarter of those who use Teams for this purpose said they trust it.

These respondents are knowingly taking a chance, gambling that they will not be breached or compromised.

The differences in usage and trust raise interesting questions about why people don't use secure tools all the time. They undermine respondents' claims that their organizations provide appropriate communications tools and that sensitive communications are secure. For organizations that conduct high-consequence communications, this contradiction cannot be ignored.

**Which of the following tools do you use, and which do you trust the most to communicate confidential, classified, or other highly sensitive information?** *(Select all that apply)*





# SECU-RITY

## The Boundary Is The Weak Point

Beyond internal security hygiene, the research reveals other significant challenges when sensitive communications leave organizations and extend to customers, partners, and vendors. At least nine in 10 (**93%**) respondents see at least one risk in common communications tools when talking with outside partners, and half express concerns.

Top risks include:

- **50%** Legal Liability
- **39%** Non-compliance
- **37%** Partner Security Posture
- **28%** Not Built for Sensitive Communications

These risks lead to serious consequences. Brand damage (**37%**), job loss (**19%**), and financial losses (**17%**) top the list.

# Secure Communications Require Control and Governance

Encryption is essential, but it is only one ingredient in the recipe for secure communications.

Organizations also need to control who can participate in a conversation, what information participants can access, how long that access lasts, and what happens to the conversation when it ends. Without appropriate controls, even encrypted communications can create liability and compliance risks, particularly when records must be retained, retrieved, or audited.

The findings underscore why this matters in practice: 2 of 5 (**39%**) study respondents identify non-compliance as a risk. The usability gap adds another layer of complexity. Combined with the earlier finding that **84%** of respondents who are non-compliant with using sanctioned communications tools for sensitive conversations say alternatives are more user-friendly, it becomes clear there is a gap between security and how people communicate in practice.

When sensitive information moves between agencies, organizations, and departments, participants may operate under different security policies and regulatory obligations.

Secure communications must go beyond protecting messages in transit. Organizations must verify participants, govern access across devices and organizations, and maintain appropriate control over records and security policies throughout the communication lifecycle.

Encryption protects the message. Governance helps keep high-consequence conversations controlled and compliant.

# AI and Quantum Add New Complications

Organizations are tasked with implementing secure communications policies and practices amid rapidly evolving threats. AI undoubtedly introduces new threat activity and enables bad actors to be more efficient and effective, adding to the traditional risk landscape.

Unsurprisingly, unauthorized outside access is cited as a chief concern for 3 of 5 (**62%**) respondents. More than half (**55%**) say AI threats are a concern too, followed by communications with outside partners (**50%**) and insider threats (**44%**).



AI ushers in a new wave of concerns, from misinformation to deepfakes and a general lack of awareness. These threats present major challenges for teams accountable for protecting sensitive communications. They must be able to answer questions that include:

TODAY

Unknown
Who actually sent this? 9:41 PM

Is this person who they claim to be? 9:41 PM

Is this content authentic? 9:42 PM

Has the message been manipulated? 9:42 PM

Can the recipient verify its source? 9:43 PM

Quantum computing's emergence further escalates risks, threatening traditional encryption methods. When AI and quantum converge, the threat landscape expands. Research shows organizations are not prepared and some are not even aware of the looming threats.

For example, more than half of government respondents (**58%**) say they are not at all familiar with quantum-safe solutions, which is higher than the study's industry average (**36%**). New threats posed by AI and quantum also leave respondents uncertain. Just **35%** say they are very confident that security solutions can adapt to new AI and quantum computing threats.

Can existing security solutions actually "adapt" to quantum and AI threats through incremental updates, or will organizations ultimately require AI-native architectures designed to stop the new class of threats?

**# ai-risk** 500 members

AI **Survey** 9:41 PM
Which AI-related threats are you most concerned about when securing confidential, classified, or other sensitive communications?
*(Select all that apply)*

59% AI-Generated Malware

54% Disinformation/Misinformation

50% Deepfakes

41% Lack of Awareness of AI Risks

39% Difficulty Verifying Identities or Content

34% Lack of Transparency in AI

500 replies · Last reply today

# DEFENSE

Of the five industries, military and defense show some of the biggest communications security gaps, even with some of the highest stakes and levels of security awareness.

Confidence can sometimes be inflated, with reported behaviors showing a mismatch. Slightly more than a quarter of respondents in the sector admit to occasionally using communications tools that do not meet security requirements, marking the highest rate of any industry. Fewer than three in five respondents say their employees always use appropriate tools, and **11%** believe their employees use appropriate tools sometimes. Inconvenience is the leading reason why sanctioned communication tools are not used regularly.

What makes these findings stand out is not that the defense sector is less aware of secure practices. In fact, these respondents demonstrate the greatest awareness of emerging threats, and they're most likely to use a tool like Signal, which incorporates end-to-end encryption, for secure communications. However, this awareness does not always translate into compliant behavior: More than one in four (**28%**) still use non-compliant tools at least some of the time.

The gap between awareness and everyday practice is especially concerning in a sector where compromised communications can have consequences that extend far beyond data loss. One in five defense respondents identify loss of life as a potential consequence of compromised communications. This underscores the gravity of their responsibility. That responsibility can take a personal toll, with respondents reporting anxiety (**39%**), difficulty sleeping (**23%**) and strained professional relationships (**22%**) as a result.

**1 IN 5**

identify loss of life as a potential consequence





## The Human Cost Of Accountability

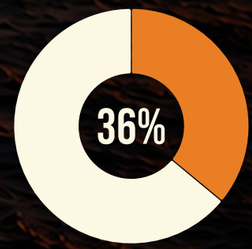
Amid the pressure of securing high-consequence communications that cannot be compromised, another risk lurks in the background, often unseen and often unknown. When it emerges, it may be too late. The risk involves more than data, information, or plans. It even extends beyond financial and organizational stability.

**That risk is the toll that securing sensitive communications takes on people.** The burden of protecting others amid high-consequence, high-intensity situations creates pressure most humans rarely experience, especially when lives or fortunes are at stake. From IT and security to logistics and operational personnel, the pressure affects them deeply.

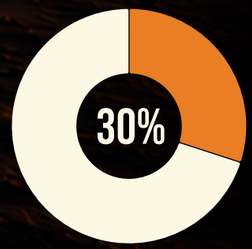
As the study reveals, the mission to secure sensitive communications takes on an added objective to protect those who protect others. Support teams need better tools.

At least 3 in 10 respondents grapple with increased stress (**36%**) and anxiety (**30%**). The cause-and-effect flywheel cascades from there. The stress leads to one in 10 admitting adverse effects on their physical health (**10%**), difficulty sleeping (**12%**), low morale (**12%**) and strained relationships with co-workers, spouses, families, and friends (**10%**). These outcomes cause **11%** respondents to question their career choice.

### THE PERSONAL TOLL




*Grapple with increase of stress*




*Grapple with increase of anxiety*

**Difficulty Sleeping** 12%

**Adverse Effects on Physical Health** 10%

**Strained Personal Relationships** 10%

# Security Is a Shared Responsibility

While most respondents believe their organizations expect them to be accountable for securing sensitive communications, the research reveals another telling theme: **They are not alone**.

Although a majority (**70%**) agree that IT is accountable, the research results make it clear that protecting people and sensitive communications is shared across multiple personas. Almost half of respondents believe executive teams (**46%**) and managers (**48%**) share the burden. Two in five believe CEOs (**41%**) do too. Three in 10 call out boards of directors (**31%**).

Beyond user-based organizations, one in three (**35%**) say vendors that provide secure communications tools are also accountable, and **23%** point to telecommunications providers.

When this many respondents call out product vendors, telcos, and leaders, it signals that times are changing. Malicious actors probe for the weakest link, whether it is in a cellular network, a product vulnerability, or human behavior. They do not care where they can infiltrate and achieve their mission. Study respondents indicate that the ecosystem that makes up secure communications – from providers to users – shares accountability and must work closer together.




# From Security Intent To Security by Design

Across industries, leaders need to ensure the secure option is also the usable option. Organizations should choose security products that are fast, easy to use and ultra-secure. This eliminates the need for employees to choose between ease/speed and security. Usability must be treated as a security requirement, not an afterthought. This requires leaders to do the following:

## Security by Design

Usability is a security requirement, not an afterthought.

**Define clear boundaries for sensitive communications**
Employees need a clear distinction between everyday collaboration and communications requiring heightened protection.

**Extend security, compliance, and governance across organizational boundaries**
Controls should follow sensitive conversations when they move to partners, contractors, customers, and other external parties. Organizations should evaluate whether their communications solutions support appropriate access controls, supervisory oversight, auditability, and policy enforcement, not simply whether messages are encrypted. These capabilities should support legitimate collaboration without adding unnecessary friction, and all parties should hold each other accountable for maintaining appropriate security standards.

**Build for authenticity and confidentiality**
AI-generated content, impersonation, and deepfakes make identity and content verification increasingly important. The human element remains the most common point of compromise in data breaches, and new tools make attacking this part of the threat surface easier than ever.

**Design for emerging threats**
Avoid bolt-on solutions and patchwork fixes. Agility is also key; having systems with flexible and/or redundant protection is essential in a constantly evolving threat environment.

**Treat security as shared accountability**
IT and security teams cannot carry the entire burden. Leadership, employees, vendors, service providers, and partners all contribute to the secure communications ecosystem.

**Build guardrails that protect users**
Even when the stress and urgency of a situation causes them to forget or ignore their security training.

ENCRYPTED · VERIFIED · GOVERNED



1 of 128

**Research Team** <research@example.com> Sep 30, 2026, 9:41 AM
to me

# Moving to a More Secure, Compliant Communications Future

Across regulated industries, organizations acknowledge the importance of securing sensitive communications. Almost all respondents believe their confidential communications are secure and that they have appropriate tools in place.

However, these perceptions tell only part of the story. Respondents don't always follow security policies, and they use non-compliant tools for sensitive communications. A disconnect exists between how strong organizations think their security is and what everyday communications practices reveal.

Even encryption is not a silver bullet. Organizations need to understand whether sensitive conversations remain appropriately controlled and documented in practice, especially when they cross organizational boundaries. Inconvenience, comfort with alternative tools, and the perceived complexity of sanctioned solutions can undermine even well-designed security programs.

Secure communications must be treated as a technical priority and a standard part of how work gets done. Organizations must delineate secure communications channels from convenient everyday tools that do not meet security requirements. Safeguards and access controls must support legitimate business needs without adding unnecessary friction.

At the same time, organizations must not assume that today's safeguards will automatically meet tomorrow's requirements. AI is introducing new threats, and quantum computing casts doubt on the long-term adequacy of today's security infrastructure.

To succeed today and in the post-quantum era, organizations must align their security investments with human behavior, operational realities, and emerging risks. Those that do will be better positioned to protect not only their information and reputation, but also the people and missions that depend on trusted communications.