PATHFINDER REPORT


# Growing Use of Consumer Messaging Apps Exposes Organizations to Privacy, Compliance and Security Risks

OCTOBER 2017

COMMISSIONED BY

## About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

## About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.



**NEW YORK**
1411 Broadway
New York NY 10018
+1 212 505 3030

**SAN FRANCISCO**
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

**LONDON**
Paxton House
(Ground floor)
30, Artillery Lane
London, E1 7LS, UK
P +44 (0) 207 426 1050

**BOSTON**
75-101 Federal Street
5th Floor
Boston, MA 02110
Phone: +1 617.598.7200
Fax: +1 617.357.7495

# EXECUTIVE SUMMARY

Employees are increasingly relying on mobile messaging in addition to traditional business communications such as email and unified communications (UC) to get their work done. 451 Research estimates that two out of three employees use a smartphone for business purposes. Of those users performing work-related activities on a smartphone, 73% use mobile messaging – including SMS/text messaging and over-the-top (OTT) consumer messaging apps – for business purposes, according to our Voice of the Connected User Landscape (VoCUL) service.

Mobile messaging can be an efficient real-time collaboration tool that enables organizations to improve productivity. However, the lack of a secure enterprise-grade messaging solution prevents many organizations from taking full advantage of mobile messaging's benefits. Furthermore, organizations tend to be lax regarding the use of personal devices and non-sanctioned apps for workplace communications. They are typically unaware of the extent to which non-sanctioned applications are being used, which opens the door to privacy, compliance and security risks. Furthermore, the lack of awareness could lead organizations to underestimate the level of risk they are facing.

This Pathfinder Report provides data and analysis on the use of consumer messaging apps in the workplace before making recommendations on how to evaluate and mitigate the risks they entail.

### KEY FINDINGS

- Employees are increasingly relying on consumer messaging apps for business purposes. This indicates that a number of use cases are not being addressed by the business communications tools their organizations provide.
- Organizations are unaware of how extensively employees are using non-sanctioned apps in the workplace, opening the door to privacy, compliance and security risks.
- Many organizations are at risk because they do not have a secure enterprise-grade messaging product in place.

## Employees rely on non-sanctioned apps to get work done

**A growing volume of business communications is shifting to consumer messaging apps on mobile devices.** That said, there is no simple way to know just how much traffic is actually being displaced from traditional business communications by consumer apps such as Facebook Messenger, WhatsApp, WeChat, Line or SMS. There are several reasons for this, including the fact that these applications are outside the scope of IT and, therefore, challenging – if not nearly impossible – to track. Second, a significant portion of OTT traffic growth is the result of use cases that are not currently addressed by existing business communications offerings.

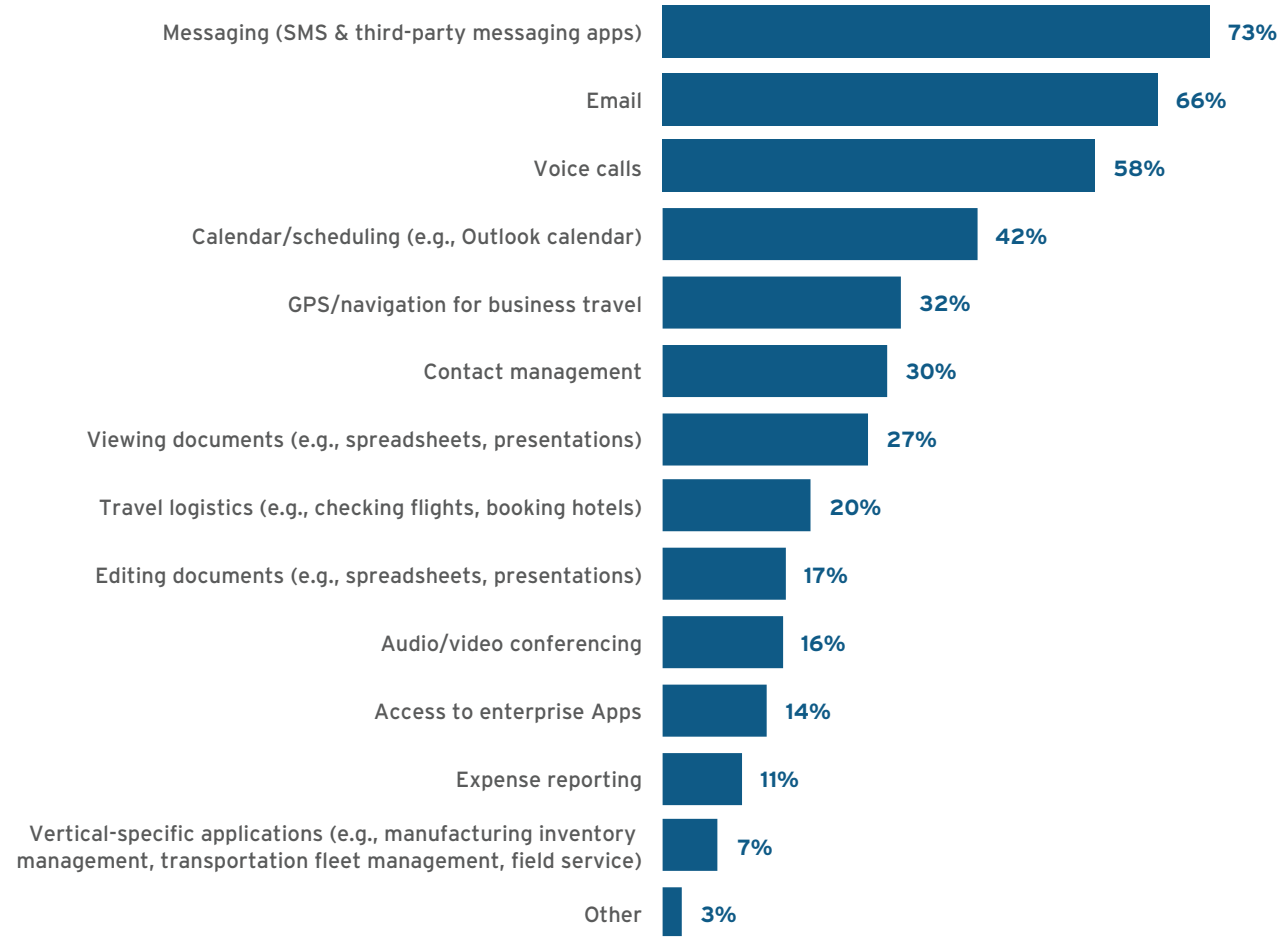
The growing relevance of mobile messaging apps for internal business communications, however, is undeniable. 451 Research's VoCUL provides evidence that employees are relying on mobile messaging in addition to traditional business communications such as email and UC to communicate with each other and with partners and suppliers.

User behavior is a key factor driving the use of mobile messaging in the workplace. In the last few years, messaging apps have emerged as one of the preferred forms of communication for consumers. They are easy to use and represent a faster, more effective alternative to email. According to 451 Research's VoCUL Consumer Representative Survey, 84% of mobile users in the US use messaging services for personal purposes.

When it comes to business use of mobile devices, our VoCUL survey results show that messaging is the top activity in the US, even above email and voice calls; 73% of survey respondents report using messaging on their smartphones for business purposes.

## Figure 1: Messaging is the top activity for employees using a smartphone for business purposes

*In which of the following ways do you use your smartphone for business purposes?*




*Source: 451 Research VoCUL Smartphones – Consumer Representative Survey, Q4 2016*

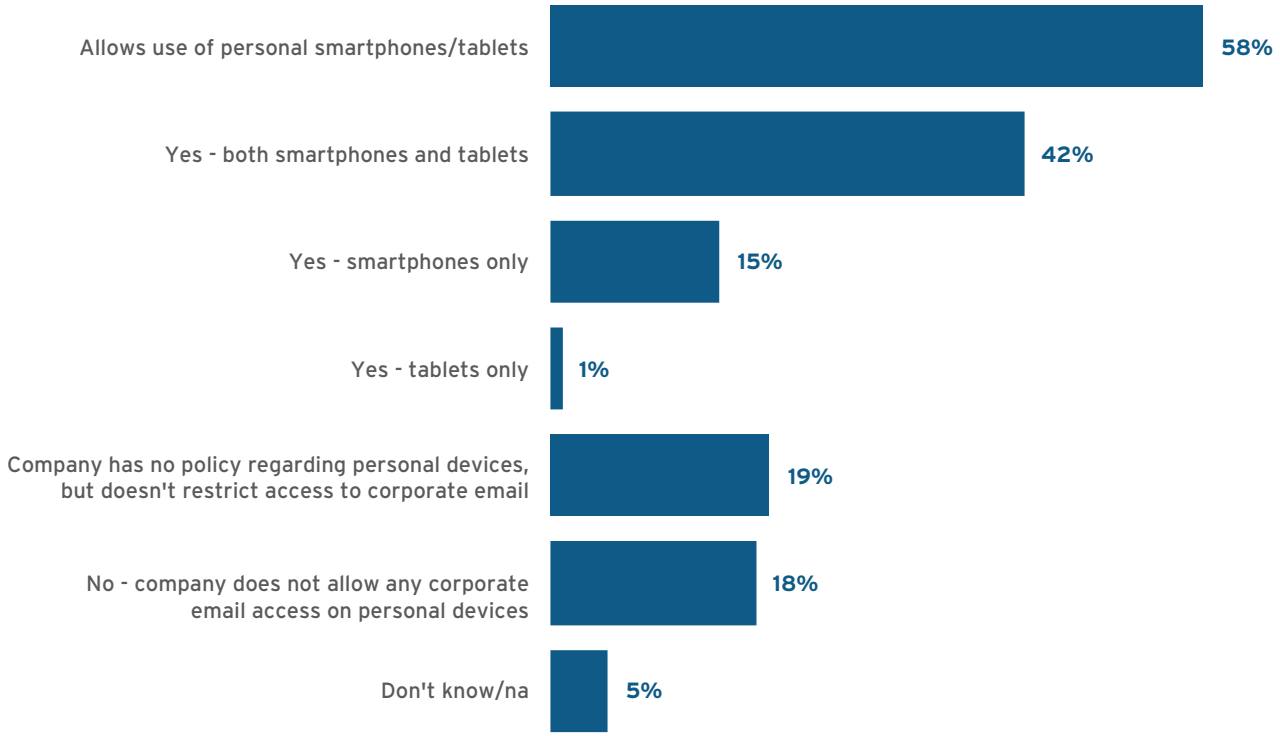
Their popularity with consumers is a key driver, but other factors are also influencing the use of messaging apps in the workplace. These include bring-your-own-device (BYOD) policies and limitations of traditional business communications products.

### BYOD PERPETUATES THE USE OF CONSUMER MESSAGING APPS IN THE WORKPLACE

According to 451 Research's latest VoCUL Corporate Mobility and Digital Transformation Survey, most companies allow employees to use their personal mobile devices for business purposes (e.g., email, connecting to the corporate network). When asked about their company's BYOD policy for mobile devices, 58% of respondents stated that their companies allow the use of personal smartphones and/or tablets for business purposes, as shown in Figure 2. Only 18% do not explicitly allow access to corporate email on personal devices, while 19% have no formal policy regarding their use.

## Figure 2: Most companies allow employees to use their personal mobile devices for business purposes

*Some companies allow employees to use their personal smartphones and/or tablets for business purposes - such as company email, connecting to the corporate network, or using other IT resources. Other companies only allow access to email and other IT resources through approved, company-provided devices. Does your company allow employees to use their personal smartphones and/or tablets for business purposes?*



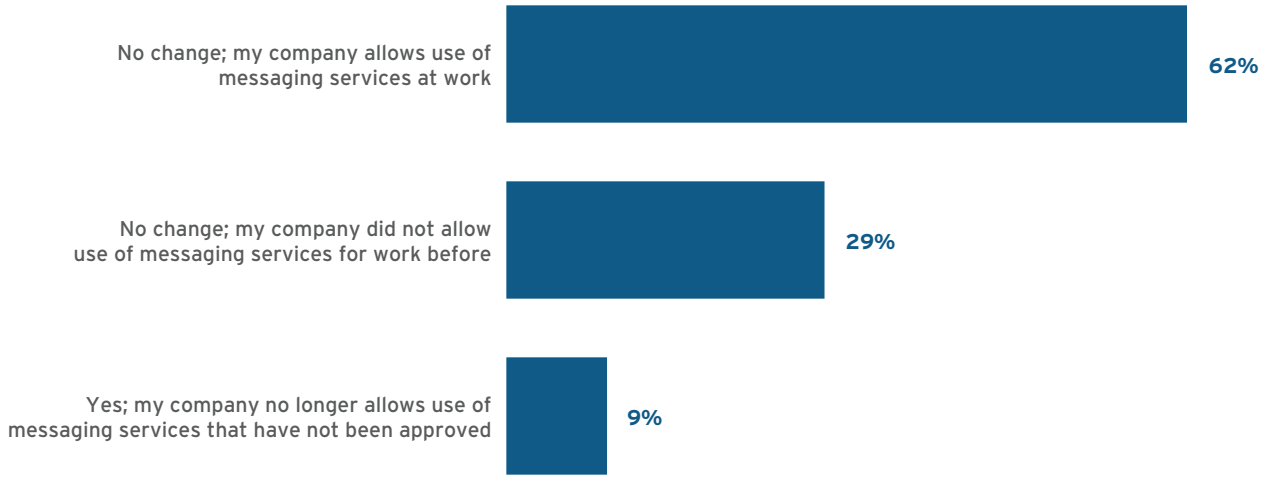

*Source: 451 Research VoCUL IT Spending Survey, 3Q 2017*

BYOD policies vary significantly by company size. Midsized companies (101-1,000 employees) are more likely to allow the use of personal mobile devices (64%). Larger companies (1,000+ employees), on the other hand, are more likely to have a strict BYOD policy: 24% do not allow the use of personal devices, and only 9% do not have a formal policy in place.

When it comes to employees' use of consumer apps in the workplace, nearly two-thirds of survey respondents said their company has not made any policy changes in the last six months regarding messaging services due to security concerns, as shown in Figure 3. Only 9% said their company no longer allows use of messaging services that have not been approved.

## Figure 3: Most companies have not made policy changes in the last six months regarding messaging services due to security concerns

*Has your company made any policy changes in the last six months regarding messaging services (e.g., SMS, Skype, Facebook, WhatsApp) due to security concerns?*




*Source: 451 Research VoCUL, Consumer Representative Survey, Q4 2016*

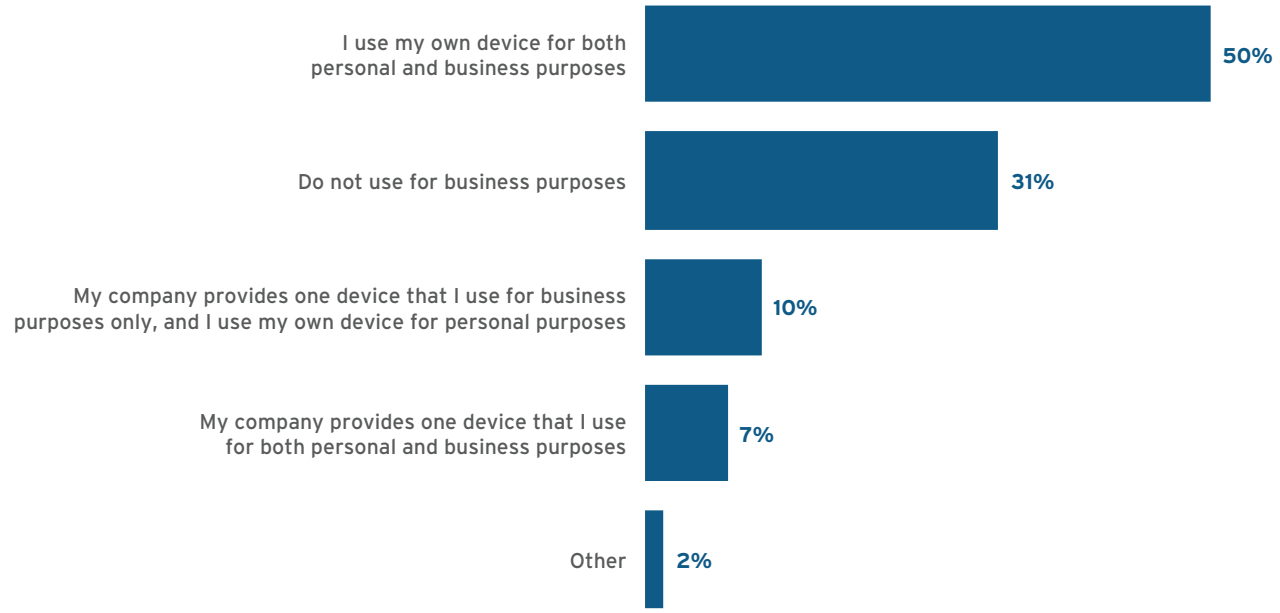
### THE USE OF NON-SANCTIONED APPS REFLECTS LIMITATIONS IN BUSINESS COMMUNICATIONS PLATFORMS

Employees are relying on consumer messaging apps in addition to traditional business communications such as email and unified communications. The former cover a wide range of use cases and have been the most important tools for communication and collaboration in the workplace for many years. They remain relevant and widely used.

However, employees increasingly use mobile devices for business communications. Survey results show that nearly 70% of respondents use a smartphone for business purposes – either personal or provided by their companies (Figure 4). Of those users performing work-related activities on a smartphone, nearly 40% report doing so on a daily basis (Figure 5).

## Figure 4: Most employees are using smartphones for business purposes

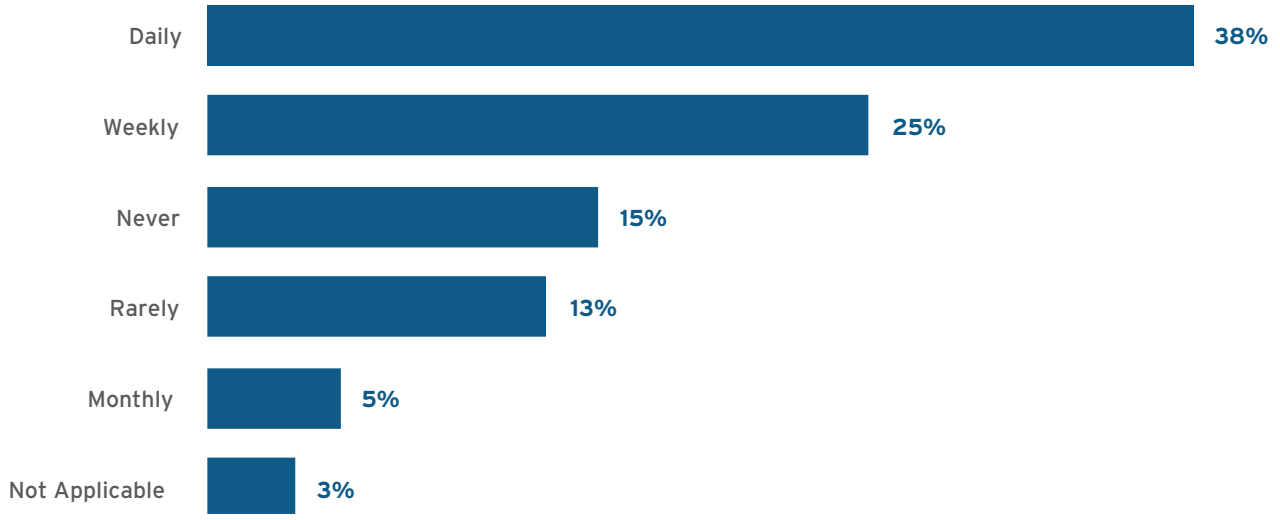
*Which of the following best describes how you use a smartphone for personal and business purposes?*




*Source: 451 Research VoCUL, Consumer Representative Survey, Q4 2016*

## Figure 5: More than one out of three employees use a smartphone for business purposes on a daily basis

*How often do you perform work-related activities on your smartphone?*




*Source: 451 Research VoCUL, Consumer Representative Survey, Q4 2016*

IT managers should consider the use of consumer messaging apps in the workplace an indication that the business communications tools they are providing their employees are not addressing many of their requirements and use cases. The apps' growing relevance in the workplace and the absence of mobile messaging in communications tools that organizations provide to their employees reflect a critical limitation in the current business communication platforms. These limitations lead employees to rely on consumer messaging apps for real-time peer-to-peer communications.

UC offerings have traditionally focused on VoIP and online meetings but – with some exceptions – not mobile messaging. In many cases, the messaging capabilities provided by UC vendors were developed for a desktop environment and are not optimized for mobile devices. This translates into a poor user experience that discourages their use. In contrast, SMS and OTT messaging apps such as Facebook Messenger and WhatsApp provide a superior user experience that have made them the most popular apps on mobile devices.

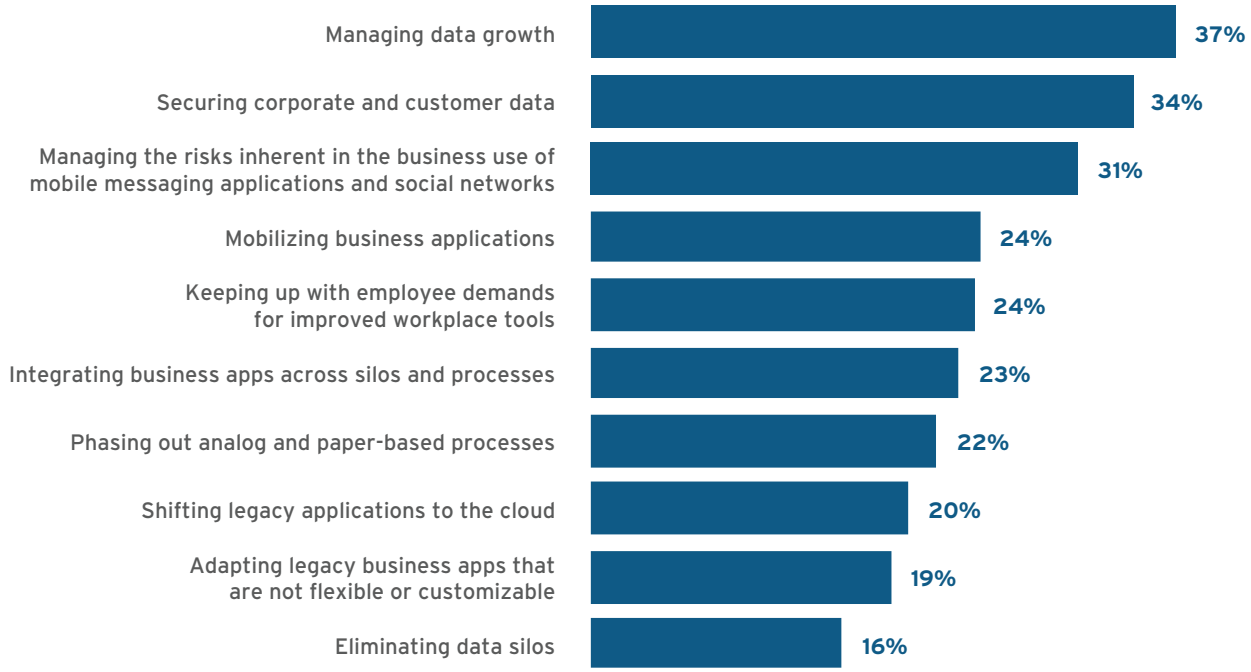
## The shift to consumer messaging apps opens the door to security risks

The shift from traditional business communications such as email and UC to consumer messaging apps opens the door to privacy, compliance and security risks that IT decision-makers did not previously have to worry about within a closed, hardware-centric environment that was completely controlled and managed by IT.

The risks these apps entail is top of mind for IT decision-makers. 451 Research's VoCUL survey results show that managing the risks inherent in the business use of mobile messaging applications is one of their top priorities, as shown in Figure 6.

### Figure 6: IT decision-makers worry about the risks that mobile messaging apps entail

*Question: What are your top priorities in terms of addressing business application software pain points? (Choose No More Than Three)*




*Source: 451 Research VoCUL Corporate Mobility and Digital Transformation Survey, 2H 2016*

**Organizations are unaware of how extensively employees are using non-sanctioned applications for business purposes.** Mobile applications are easy to use without oversight and can be quickly adopted by employees to solve business problems without involving the IT department. It follows that if organizations are unaware of the extent to which consumer apps are used in the workplace, they may also be underestimating the risks their use entails.

There are several high-risk security and compliance vulnerabilities associated with the use of consumer messaging apps for business purposes. These applications are vulnerable to unexpected leaks – accidental or intentional – of confidential data. If the device is lost or stolen, IT cannot remotely remove sensitive business information on OTT apps from the device. The lack of access management also prevents IT from blocking unauthorized use of OTT messaging apps.

In addition to data leakage, organizations in highly regulated industries such as healthcare, government and finance that deal with highly confidential and sensitive information could face significant fines given that the data within OTT apps is not adequately protected and does not have a backup system in place for auditing purposes.

The risks brought on by the use of consumer messaging apps are not limited to regulated industries. Organizations of all sizes and across different industries handle sensitive information that requires a high level of privacy and security, including information related to intellectual property, financial reports, legal discussions, R&D and M&A.

### HOW CAN IT GAUGE AND ADDRESS THEIR LEVEL OF RISK?

**IT organizations must apply the same standards for protecting the integrity of mobile messaging as other forms of corporate communications.** As with email and web browsing, mobile messaging can be subject to malware, surveillance and other forms of cyber threats. But how can organizations bring mobile messaging to the same level of security and control as email and UC? CIOs, CTOs and IT decision-makers are well aware that no single product will be 100% secure. The first step, however, should be to assess the level of risk.

Organizations should evaluate the data protection, security, compliance, productivity and business risks associated with the use of consumer messaging apps in the workplace. They do not need to track the volume of OTT traffic to evaluate their level of risk when it comes to the use of non-sanctioned mobile applications. There are several alternatives that can provide insights, including using mobile device management products to assess the number of managed devices using OTT messaging apps.

Enterprises can define policies to regulate how and when employees can access OTT apps in the workplace, and they can use networking tools to monitor and identify OTT app use when employees access their company's corporate Wi-Fi. Another option is for organizations to completely blacklist OTT messaging apps.

Finally, organizations can survey employees to gain insights into how much they are using these apps for business purposes. More importantly, this can also help organizations understand the use cases for which employees are relying on OTT messaging apps to get their work done.

## Secure messaging adds critical capabilities to business communications

The list of potential security risks associated with the use of consumer messaging applications in the workplace is a long one. Organizations should consider these risks when evaluating business communications and team collaboration technology. There are, however, other important considerations that organizations should take into account.

For example, consumer messaging apps are far from adequate when it comes to using them for business purposes because they do not support all the relevant use cases for employees, leading to ineffective communication and collaboration. Furthermore, they are not integrated with business applications, which leads to workflow inconsistencies and interruptions that can impact overall productivity.

**Many organizations are at risk precisely because they have not yet deployed a secure enterprise messaging product.** Employees will rely on non-sanctioned apps to get their work done when a secure and efficient enterprise application is not available. The abundant use of OTT apps indicates that existing business communications tools don't address a number of use cases that employees require. It might seem that the risks involved leave many organizations – particularly those in highly regulated industries – with no choice but to prohibit employees from using consumer messaging apps for business purposes.

However, secure mobile messaging can fill the gap left by email and UC by providing a secure real-time communications tool to enhance the ways in which employees interact with each other and with partners and suppliers. Organizations should consider deploying a secure enterprise messaging product to address the limitations in business communications while at the same time providing adequate security, data protection and compliance.

## Conclusions

Email and phone have been the dominant channels for business communications for more than 20 years, but there are indications this is changing. Employees increasingly rely on mobile devices in addition to traditional business communications such as email and UC to get their work done.

We do not expect mobile communications will entirely displace traditional business communications, at least in the near term. A more likely scenario is that they will coexist, with users relying on them for different purposes.

451 Research predicts that as mobile penetration continues to grow, the use of mobile messaging in the workplace will significantly expand. As usage grows, so too will threats and security risks. We expect that secure enterprise mobile messaging will emerge from behind the shadow of consumer messaging apps to become a core productivity tool that workers use on a daily basis, alongside email and calendar applications. We also expect evolving privacy and security requirements will result in secure messaging emerging as a distinct business communications category.