FROST & SULLIVAN

Insights for Chief Information Security Officers (CISOs)—Secure Messaging Solutions

Transformational Growth in Digitalization and its Impact on Communication for Business Needs

Global Security Research Team at Frost & Sullivan

The Growth Pipeline™ Company
Powering clients towards a future shaped by growth

K808-74

January 2023

Table of Contents

Author: Sarah Pavlak

Growth Opportunity Analysis—Enterprise Messaging Solutions

Communication Needs Shift as the Workplace Evolves

Business productivity practices have changed dramatically over the past several years. This is attributed to not only the move to a remote workforce but also the accelerated enterprise digital transformation. Communication, both physical and virtual, is an essential component of business efficiency. Workplace communication statistics reveal that 86% of workers attribute workplace failures to a lack of efficient communication and collaboration.[1] Personal and professional interactions depend heavily on virtual communication methods. People expect instant gratification—immediate responses to requests. This carries over into the business enterprise realm.

Enterprise messaging integrates different types of virtual communication required for businesses going through digital transformation. Workdays are no longer bound by 9-to-5 in-office schedules. Teams now work from anywhere and everywhere. Time-zone adaptability is essential to accommodate flexible working hours. Secure communications solutions must be adaptable to such changes for businesses to thrive. While traditionally email has been the most widely used virtual business communication tool, enterprise communication is now transitioning to (and becoming dependent upon) enterprise messaging solutions. Such solutions offer enterprises enhanced security efficacy, interoperability, and team productivity acceleration.

[1] "Workplace Communication Statistics (2022)", *Pumble*, https://pumble.com/learn/communication/communication-statistics/.

Benefits of Non-email Messaging Solutions

Email is—and always has been—an effective communication method. But it is antiquated and cannot meet the communication demands of today's workforce. It takes time to compose, send, and respond to emails. Employees want simpler, more convenient communication methods.[2] Enterprise messaging solutions offer easier communication for workers. For example, emails overload inboxes and overwhelm employees. Secure instant messaging apps for businesses distill communication down to more straightforward conversation, offering quicker response times, simple and informal language, and talk-to-text features. This makes communication more efficient, enabling easier multi-tasking in a secure environment.

Organizations must adapt to the expectation of instant response. Employees often deal with teams spread across multiple time zones. They want to remain connected in real time to leadership and colleagues to resolve issues quickly. Instant messaging apps offer employees the convenience of quick chat sessions. Instant chat facilitates escalation, something important for urgent communication. Ease of communication can deliver employee satisfaction and help build relationships among peers and with managers.

The Digital Transformation Movement

Work Culture Changes for the Better

The enterprise security environment has evolved. With more employees working remotely, the network security perimeter has effectively disappeared. The pandemic accelerated remote work adoption and pushed the digital transformation movement into overdrive. Driving digital transformation are key technology priorities such as mobility, cloud operability and enhancements, data accessibility, and connectivity. Digital transformation has now become imperative for businesses regardless of size or location. For CISOs of all organizational sizes, cybersecurity risks are the top concern when it comes to digital transformation.

[2] "Chat is the future of communication at work, however, we can't get to that future when our habits at work are mired in the past", *Preppio*, https://www.preppio.com/blog/chat-future-communication-work.

The workforce has moved to a remote and hybrid working model, and organizations must keep teams connected to remain competitive, effective, and efficient. For remote workers, the need to feel connected to peers and managers is essential for productivity. Enterprise messaging enables this, and the number and sophistication of business communications applications continue to grow. [3] [4]

Messaging Impacts Communication through Speed, Cost, and Immediacy

Most people use more than one device to stay connected with personal contacts. This behavior carries over into working habits as well. Virtual communication solutions offer interoperability and information transparency, which results in more effective communication practices and efficient working habits. Secure consumer messaging apps are popular for personal communications, but that does not mean they can be integrated with professional messaging. It is imperative for professional communication means to be kept separate to protect proprietary information and ensure data security. Users accustomed to personal messaging features can find most, if not all, personal messaging features in enterprise messaging solutions, but with enhanced usability and security efficacy to ensure sensitive business communications are managed appropriately.

Advantages of Secure Enterprise Messaging Solutions

When deciding on an enterprise messaging solution for an organization, CISOs need to stay away from messaging apps focused on consumer messaging. There are security vulnerabilities when employees use consumer messaging apps to conduct business. While consumer apps are effective and easy to use for the modern worker who is always connected, unapproved usage for professional business matters can create a security gap, putting business infrastructure, sensitive information, and corporate regulatory compliance at risk.

[3] "Business Communication is Growing Better with Recent Trends", *CEOVIEWS*, https://theceoviews.com/business-communication-is-growing-better-with-recent-trends/.
[4] "10 Business communication trends for 2022 and beyond", *Pumble*, https://pumble.com/blog/communication-trends/.

CISOs must consider specific security features when investing in a secure enterprise messaging solution. Using a secure messaging solution specifically tailored to business needs gives users the convenience and instant feedback they are accustomed to while also accommodating the enterprise's security needs. Security efficacy, improvements to business operations, and team productivity are the biggest factors for a CISO evaluating enterprise business messaging solutions.

Exhibit 1 below depicts the key benefits that secure messaging solutions offer.

Exhibit 1: Key Benefits of Secure Messaging Solutions

Image Source: Getty Images

Source: Frost & Sullivan

Growth Opportunity Universe—Enterprise Messaging Solutions

Growth Opportunity 1—Cross-platform Support

Employees work on (and expect to be able to work on) their device(s) of choice. Cross-platform support is critical for the modern work environment due to the demand for the ability to shift between computers, smartphones, tablets, etc. However, with many organizations adopting bring-your-own-device (BYOD) policies, employees are accessing business data from personal mobile devices without applying network protection policies. Enterprise security leaders must enable work-from-anywhere-on-any-device modes while also adopting secure communication requirements. CISOs must be equally aware of messaging solution capabilities and security features before integration into their organization. Enterprise messaging solutions must also be able to support multiple operating systems.

Growth Opportunity 2—Enterprise Messaging Data Control

Information shared amongst an organization's employees can be sensitive and contain proprietary material. Commonly used messaging apps for personal communications do not always offer full control over user data. CISOs must ensure their enterprise messaging app has the security and control necessary to prevent information theft.

Enterprise messaging solutions must include:

- Administrative control over data
- Management visibility into messaging traffic
- Policy-based controls
- Ability to modify controls based on organizational requirements

The nature of risk associated with the breach of business communication is different from the risk associated with the breach of personal communication. The damage caused by the breach of business communication is potentially greater. Strong end-to-end encryption capabilities are a necessity for any messaging solution application. Users, whether they know it or not, use encryption in personal messaging apps. Business messaging apps must have and depend on encryption. CISOs must be able to confirm/control comprehensive encryption. End-to-end encryption does not automatically guarantee data protection and privacy. Some messaging apps ensure encryption only during transit; therefore, an application that encrypts data both in motion and at rest must be chosen.

End users often hold on to their messages for an extended period. Encryption for data at rest ensures information remains safe in saved messages. CISOs must keep data secure and control access to messaging with multi-factor authentication and role-based permissions.

Growth Opportunity 3—Centrally Managed Platform

A centrally managed platform is a master portal for security personnel to manage enterprise security protocols across an organization. A centrally managed platform for enterprise messaging solutions offers many benefits, such as the protection of sensitive data, intellectual property security, and risk mitigation. Cybersecurity risk is now business risk: the average data breach costs a company USD$4.35M.[5] CISOs must determine how to best posture their organizations to avoid becoming the next cybercrime victim. Using a secure messaging solution that offers a centrally managed platform helps organizations stay ahead of cyberattacks because it obtains full control and transparency over what is happening with its data.

Not only is it important for the organization to own the data that is present in the messaging apps, but also for the information technology (IT) personnel to be able to control the entire communication ecosystem. Trusting data to massive communications services and consumer messaging apps opens the door to exploitation of that data because an organization does not have full control over it. This will prove to be catastrophic in the event of an attack as the provider could hold the data hostage due to ransom demands from the threat actor.

[5] The cost is even higher for healthcare providers, for which the average data breach costs USD$10.1M. See https://www.ibm.com/reports/data-breach.

Exhibit 2 below depicts the impact of digitalization on communication.

Exhibit 2: Impact of Digitalization on Communication

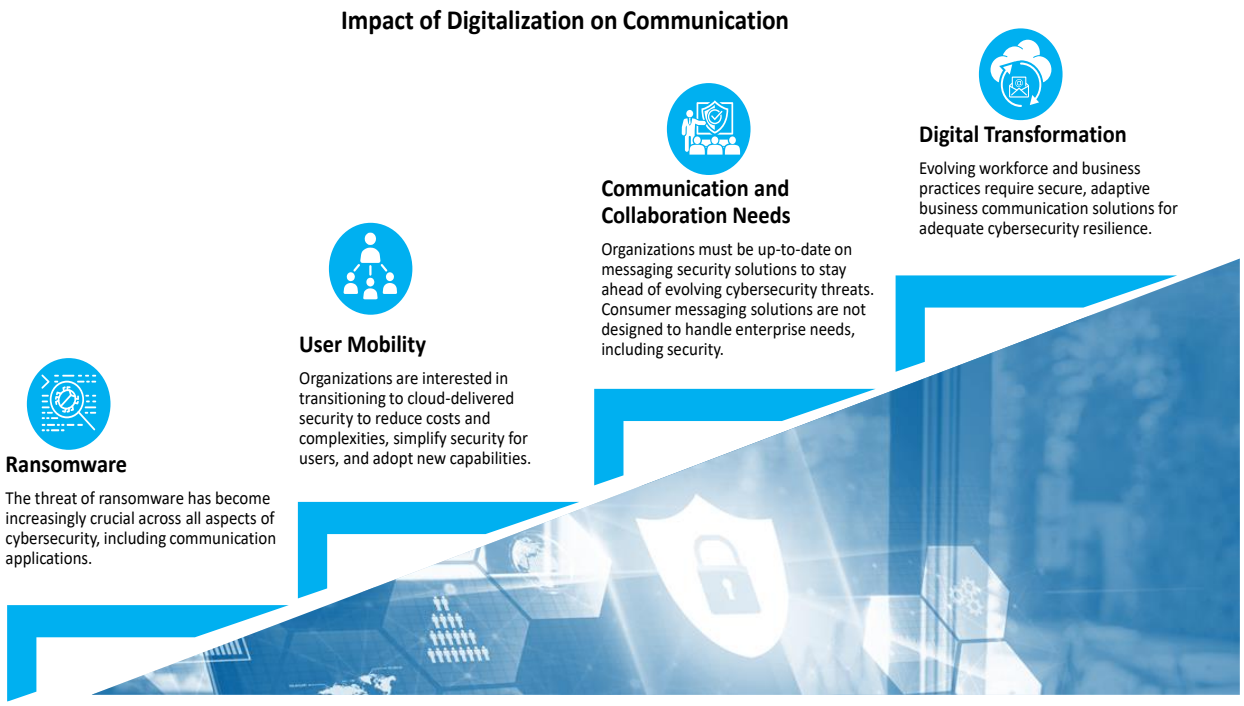

Image Source: Getty Images

Source: Frost & Sullivan

The Final Word

The communication needs of organizations will continue to evolve. CISOs must be ready to adapt without losing their steadfast focus on cybersecurity posture, data security, and control. Enterprises must adapt their corporate communication methods to meet changing expectations. And those expectations change based on the performance of unsecured communication applications.

The threat landscape continues to evolve rapidly, presenting a significant challenge for cybersecurity solution vendors. As attackers become more sophisticated, enterprise messaging solutions must evolve to block new attacks. The enterprise shift to remote work has introduced new vulnerabilities for users and organizations. Threat actors have taken advantage of new, more sophisticated cyberattack modes, particularly targeting email. Messaging apps are their next target. CISOs must act now to establish relationships with trusted secure messaging solutions providers, ensure data encryption for messaging data in transit and at rest, and optimize corporate messaging performance to meet user expectations.

As part of the research for this insight, Frost & Sullivan spoke with leading cybersecurity experts, including Retarus, Element, NetSfere, Haiilo, Mattermost, and Rocket.Chat to examine different secure messaging solutions and associated security trends and challenges.

Growth Pipeline Engine™

Frost & Sullivan's Growth Pipeline Engine™ supports clients through all 5 phases of growth: from developing, evaluating, and prioritizing opportunities to building and implementing go-to-market strategies and optimizing opportunities. The objective of this study is to be a client's first step on a growth journey.

FROST & SULLIVAN

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com