FALL 2021 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, computer forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss the growing business messaging application market, eDiscovery nuances and relevant court cases.

Business Messaging Applications:
Productivity Trick or Treat?

Distributed workforces have rapidly evolved over the years, and we've seen this process accelerate with the COVID-19 pandemic. This exponential increase has been a boon for business messaging app developers such as Slack, which originally launched as an internal tool back in 2013. Since then, we have seen further competition and an expansion of features and integrations, which has opened a world of remote collaboration. The top three market leaders, Microsoft Teams, Google Chat (formerly Hangouts), and Slack, dominate the estimated $13 billion-dollar global market for these applications (https://www.statista.com/outlook/tmo/software/productivity-software/collaboration-software/worldwide). But what exactly are these organizational communications apps? How do they function? And what are the associated risks? In short, are business messaging apps productivity treats helping organizations revamp their workflow or tricking us into storing our data in a single, vulnerable environment?

Whether labeled as a business messaging app, an enterprise communications app, or a team messaging and communications app, this category of application is designed to enhance the speed and efficiency by which collaborators work. An organization's employees and external partners can connect through a single administered space with popular, useful functions such as text/SMS/MMS/instant messaging, segregated group spaces, audio/video calls, file transfer and sharing, task management, and in some cases, screen sharing. The structure of each app's form and function is unique, although Slack has engaged in litigation over design elements being infringed by others.

For many organizations and employees, this centralized hub makes remote office and work from home arrangements easier by allowing them to communicate in real time and

asynchronously from a single app and/or from multiple devices without a lot of extra screen swapping. Users can work together on-screen while monitoring live-chat on other projects within the same app space. The delay inherent with email is all but eliminated when your co-workers, vendors, or clients are able to jump into a relevant conversation at any time. Understandably, participants in vastly different time zones will be adding to the exchanges according to their work hours, but for those business messaging apps that included threaded message formatting and customized notifications, the discussions and contributions of those who work in far-remote locations are not lost or buried in the accumulated data.

What's not to love about an app that combines the speed of instant messaging, the efficiency of shared calendaring, and the convenience of a collaborative workspace? Doesn't that solve all the drawbacks of the demand for remote work arrangements? Unfortunately, like so many technological advances, the enterprise communications apps are only as secure as users are compliant with and diligent about security practices. Social media giant Twitter found out the hard way when, in 2020, hackers were able to socially engineer their way past Twitter administrators and into the company's Slack channels, where they discovered a plain text file that led to them eventually taking over the Twitter accounts of some very famous people, including former President Barak Obama, and posting links for a cryptocurrency scam. Slack was quick to remind users to never post sensitive data in open channels, but still, that warning is only good until the first employee disregards it.

Other factors that should be considered by organizations considering a business messaging app include encryption protocols, data residency, and data loss prevention. At Digital Mountain, we advocate for all data to be end-to-end encrypted, meaning that data is encrypted in transit and at rest, especially when that data is being stored on a third-party, often cloud-based, server. There are business messaging apps that are offered as local area network applications which reside on company-owned servers; however, the array of features and integrations is less than those offered with cloud-based products. Researching the potential provider's encryption practice is easily done and worth the time required, as is finding out if the provider offers data residency outside the US. Many organizations which deal with data being distributed globally may wish to consult with experts on data residency as to where in the world their data is not only safest, but also meets the regulations of various industry and government agencies.

Data shared by and stored in business communication apps is discoverable and needs to be treated as such. Like email, data loss prevention is vital and often required under state and federal regulations, especially for medical and financial data. Waiting until a preservation order happens is not the time to make sure that the provider has adequate data loss prevention measures in place. Business messaging apps may seem like just the treatment your organization needs to enable your workforce to thrive, but don't get tricked by fancy features and attractive integrations. Digital Mountain can help organizations determine if potential or current providers are doing the work necessary to protect your organization's data. Consulting with an expert like Digital Mountain before adopting an enterprise-wide communication, collaboration, and data-sharing solution may prevent a future breach or data loss scare.

Please direct questions and inquiries about electronic discovery, computer forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

TECHNO SECURITY & DIGITAL FORENSICS CONFERENCE
San Diego, CA: October 25-27, 2021

SEDONA CONFERENCE WORKING GROUP 11 MIDYEAR MEETING 2021
Houston, TX: October 28-29, 2021

INTERNET OF THINGS WORLD
Santa Clara, CA: November 2-4, 2021

ISSA SHOW 2021
Las Vegas, NV: November 15-18, 2021

OPENTEXT WORLD 2021
Virtual: November 16-18, 2021

Click here to see more upcoming events and links.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: