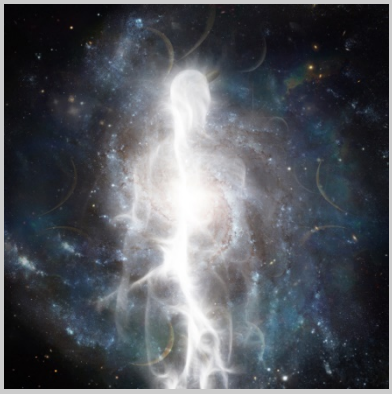
FALL 2020 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, cybersecurity and data analytics needs. For this E-Newsletter, we focus on ephemeral communications and the affect of disappearing messages on discovery cases.

Implementing Organizational Ephemeral Messaging App Use: Not Everybody Should



The rush to adopt the latest trend can often lead to misgivings – whether it's just the embarrassment of a mullet haircut or the danger of something like ingesting a laundry pod, jumping on a trend is often a mistake. Tech trends are no exception – they can lead to unwanted consequences if not examined carefully before adopting. Ephemeral messaging apps (EMA) being used for secure communications by organizations is just one such trend that could probably benefit from some examination. Impetuous adoption could lead to a loss of valuable information and may, for some organizations, amount to a violation of industry regulations. When your employees are pushing for EMA permission, how you proceed may be the difference between wise adoption of new technology or a host of regrets.

Not a Good Fit for Finance

In December 2018, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations issued a Risk Alert that warned that any organizations covered by the Investment Advisors Act of 1940 should avoid the use of EMA (https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf).

More recently, the Financial Industry Regulatory Authority (FINRA) reached a settlement with an industry member who used WhatsApp to conduct securities related business without preserving records as required (https://www.finra.org/sites/default/files/fda_documents/2018059746001%20Paul%20A.%20Falcon%20CRD%202464566%20AWC%20sl.pdf).

The resulting 30-day suspension and five thousand-dollar fine may seem inconsequential, but underscore the idea that FINRA is not averse to investigating the use of EMA by industry

members. Financial organizations that wish to take advantage of EMA technology would be wise to consult with experts on both the technology and the regulations to avoid walking the wrong side of an exceptionally fine line.

Setting the Rules and Permissions

Organizations that do want to take advantage of the benefits of EMA should begin with thorough investigation and planning to ensure a good fit with the organization's goals. If systematic, policy-driven data reduction is desired, then choosing an enterprise-based app with administrator-set retention and deletion settings is going to be high on the list of criteria. Enterprise-based apps can include features such as the ability to centralize messaging archives and mobile device management functions to facilitate control over both data and devices – an especially important consideration for IT shops with Bring Your Own Device policies. Organizations operating under BYOD policies are still responsible for ensuring that data is stored securely when required even when employees are using personal devices.

When data security is the goal, administrators should have a solid understanding of more than any industry-specific regulations, but also an understanding of the true levels of security offered by the various apps. Ephemeral messaging apps promote the idea of data security through automated deletion and destruction; however, digital forensics practitioners have found various ways to capture data from an ephemeral app. If the app is set to retain messages after viewing, investigators with unfettered access to the device can often employ well-known imaging techniques to preserve and analyze data or resort to screen captures when technical limitations exist.

Most users of EMA set the app to shred data at the first possible opportunity. Even then, all hope of recovery isn't lost – many users sync their mobile devices to cloud-based storage or other devices, such as a PC or laptop. EMA can store data in more than one place, especially when devices are synced to cloud-based storage. With the proper tools and techniques, an accomplished digital forensics examiner can extract keychain data and unlock encrypted file data, including data that may have been wiped from the primary device but resides in cloud storage or as part of a backup on a secondary device. While not an easy or necessarily rapid process, the method has worked with the most secure EMA and all operating systems to date, giving rise to the concern that organizations relying on EMA to provide total data security should think twice.

For all the precautions with which an organization should approach ephemeral messaging apps, there is truth in the advertising – they do, for the most part, reduce data and increase security by automatically deleting and destroying data as promised. Knowing the ins and outs of exactly when and how that data is destroyed is something that an organization should know and be comfortable with before adopting the trend.

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

UPCOMING INDUSTRY EVENTS

THE SEDONA CONFERENCE WORKING GROUP 1 ANNUAL MEETING 2020, VIRTUAL
October 28-29, 2020

DATA CONNECTORS GREAT LAKES VIRTUAL CYBERSECURITY SUMMIT
November 5, 2020

FORENSICS@NIST 2020, VIRTUAL
November 5-6, 2020

THE SEDONA CONFERENCE WORKING GROUP 12 ANNUAL MEETING, VIRTUAL
November 9, 2020

OPENTEXT ENFUSE ON AIR 2020, VIRTUAL
November 10, 2020 - December 1, 2020

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. In the short term, she is available for webinars and remote e-conferences.

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: