MICRO FOCUS

Flyer
Retain Mobile

Top Five Reasons to Archive Mobile Communication

Why archive mobile communications? Increased mobile device data, employee misuse, and data leakage are just a few of the reasons.

By the end of 2013, the number of connected mobile devices will exceed the population of the Earth. Tablets and smartphones are changing the way users in your organization get information and collaborate. Employees are happier and more productive when they're given mobile corporate access. Businesses that go mobile gain the competitive advantage and drive top-line growth. With the increase in usage of mobile devices, organizations need to be prepared for the risks associated with mobile communications. To mitigate these risks, ensure proper use, and protect from future litigation, it is imperative that organizations archive their mobile communications.

Outlined below are the top reasons that archiving is a must:

1. A Rapid Increase in Data Being Created by Mobile Devices

- **Average smartphone usage grew 81 percent in 2012.** The average amount of traffic per smartphone in 2012 was 342 MB per month, up from 189 MB per month in 2011.
- **In 2012, the number of mobile-connected tablets increased almost three-fold to 36 million, and each tablet generated 2.4 times more traffic than the average smartphone.** In 2012, mobile data traffic per tablet was 820 MB per month, compared to 342 MB per month per smartphone
- **Android data levels are now higher than iPhone data levels in use.** By the end of 2012, average Android consumption exceeded average iPhone consumption in the United States and Western Europe.
- **Global mobile data traffic will increase 13-fold between 2012 and 2017.** Mobile data traffic will grow at a compound annual growth rate (CAGR) of 66 percent from 2012 to 2017, reaching 11.2 exabytes per month by 2017.
- **Global mobile data traffic grew 70 percent in 2012.** Global mobile data traffic reached 885 petabytes per month at the end of 2012, up from 520 petabytes per month at the end of 2011.
- **By the end of 2013, the number of mobile-connected devices will exceed the number of people on earth.** By 2017 there will be nearly 1.4 mobile devices per capita. There will be more than 10 billion mobile-connected devices in 2017, including machine-to-machine (M2M) modules exceeding the world's population at that time (7.6 billion).

2. Employee Misuse of Mobile Devices

Mobile devices have blurred the line between work and personal life. It has become more commonplace for an employee to use the same device for both personal and corporate use. This mixed usage can cause sticky situations, as organizations may be less able to manage their content. An employee could easily:

- Share sensitive or confidential information
- Participate in inappropriate, harmful, or harassing communications

3. Organizational Data Leakage

Mobile devices are increasingly becoming a key security risk for enterprises as employees use their devices to access sensitive company information. However, as the 2011 McAfee and Carnegie Mellon University survey found, most employees are not thinking enough about protecting corporate data when using these devices. Here are a few more findings from the survey.

- **One in three employees** polled kept sensitive work-related information on their mobile devices.
- **Two-thirds of employees** were not aware of their organizations' policies, even though 95 percent of companies have mobile-security policies in place to protect enterprise data.

- **Most of the companies** reported that their employees do not understand how permissions and other access settings work on their mobile devices.
- **63 percent of work-issued mobile devices** were being used by employees for personal activities.
- **About 40 percent** of the companies participating in the survey had experienced the loss or theft of mobile devices and nearly half of those devices contained "business-critical data."

In addition, employees use corporate and personal mobile devices for collaboration, whether it is text messaging, email or phone calls. Sensitive or confidential information can easily be shared via these devices. Organizations must have oversight on what employees communicate via these mobile devices.

4. Burden of Regulation Compliance

The majority of organizations do not archive mobile messaging content, despite its requirement through regulations. Court decisions and other regulations provide guidelines which indicate that this content should be archived.

The following examples highlight, by industry, a number of regulations for mobile messaging archiving and usage.

FINANCIAL

- FINRA 07-59 states that a firm's electronic communication, including instant messages and text messages, are subject to overall supervisory review and procedures.
- FINRA 11-39: Firms are required to retain, retrieve, and supervise business communication regardless of whether they are conducted from a work-issued device or personal device.
- SEC 17a-4 states that all communication must be maintained, retained, and available to be produced. This regulation was amended in 1994 to include electronic communication.
- MiFID: A European Union law that states that all electronic communication in regards to securities orders must be recorded.
- FSA: The United Kingdom published rules requiring firms to record and store relevant communication for six months.

GOVERNMENT

- 5 U.S.C. § 552, As Amended by Public Law No. 104- 231, 110 Stat. 3048 (The Freedom of Information Act): Government agencies shall make available copies of all records, regardless of form or format. Government agencies must archive all communication data to ensure that if a request is made, this data can be produced. This applies to all electronic communications, whether it is email, social media or mobile communication.
- "Sunshine Laws": These laws, which can vary from state to state, require governmental entities to capture and archive mobile communication data.

EDUCATION

- Family Education Rights and Privacy Act (FERPA): A Federal law giving students and parents the right to inspect and review the student's education record and can apply to mobile messaging data.

HEALTHCARE

- HIPAA laws state that mobile communication data must be safeguarded and archived if confidential patient information is transmitted via mobile devices.
- HITECH expands on HIPAA and holds healthcare organizations to a higher level of responsibility for breach of patient information.

OTHER ORGANIZATIONS

- The FRCP relate to the rules of discovery pertaining to electronic records search and retention in regards to eDiscovery. These rules establish that electronic communication is discoverable.

5. Policy Enforcement

Employee mobile device usage brings many benefits.

- Increased efficiency and morale
- Improved communication and collaboration
- Reduced costs when employees are using their own devices

The benefits of mobile device usage outweigh the risks; however, organizations must implement policies to mitigate risks. Policies must outline what is and is not appropriate use of mobile devices. Policies must be clear and employees must be trained on them. By implementing an effective policy an organization is on its way to being protected from mobile device misuse. But policy is not enough. There needs to be a way to enforce policy.

Archiving mobile communication gives organizations oversight for all mobile communication data. By easily accessing text messages, multimedia messages and phone call logs, you can quickly see whether employees are complying with your corporate policies. An effective archive of mobile usage gives companies the ability to enforce policies.

RETAIN MOBILE ARCHIVING

Retain™ Mobile delivers secure, encrypted messaging and archiving for iOS, Android and BlackBerry devices. This solution is for organizations that utilize personal employee and corporate devices to generate and consume business data, while meeting regulatory and compliance requirements.

Retain archives SMS/MMS, BBM Enterprise and phone call logs for Android, and BBM, BBM Enterprise, PIN, SMS/MMS and phone call logs for BlackBerry. Additionally, Retain archives all encrypted SMS/Text messages and dedicated business phone number data for iOS and Android, via the secure communications server, as well as BBM Enterprise. This means there is no need to tether or sync the device and archiving is done in real time. Retain is the only enterprise-ready archiving solution for iOS, Android and BlackBerry devices.

With Retain Mobile you don't lose valuable information and your organization stays compliant. Your sensitive data stays securely within your organization.

Information herein obtained from the Cisco Whitepaper, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017" published February 2013—**www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf**

Also see the *eWeek* article "Mobile Device Data Losses Pose Rising Security Risk: Security"—**www.eweek.com/c/a/Security/Mobile-Device-Data-Losses-Pose-Rising-Security-Risk-Survey-515021/**

www.microfocus.com

Micro Focus®
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com