AVANSIC®
eDiscovery + Digital Forensics

Updated Bring Your Own Device

By Dr. Gavin W. Manes, CEO of Avansic

Introduction

Bring Your Own Device has some new implications in the current world of remote work. The intersection between people's personal and business devices is blurrier than it has ever been. With more people working from home or spending less time at the office, many personal cell phones, computers and tablets now have much of the business data that would have previously been carefully separated. For companies and firms that did not have robust Bring Your Own Device policies and procedures, the last few months have been a crash course in implementation of them. For those that had policies, this has been a time to revisit those and make them more robust.

Another consequence of remote work is that collaboration software use is on the rise, with programs like Microsoft Teams and Slack filling the gaps for in-person meetings and group projects. Increased use of these programs will lead to the need to collect them for eDiscovery purposes, and it also brings a new set of security issues to the table.

Continued remote work also has implications for eDiscovery since devices to be collected will most likely contain personal data. In this paper, we will review a few key parts to include in Bring Your Own Device policies, provide an update on collection capabilities of mobile devices, and discuss some of the security measures for the increased use of Teams and Slack.

Bring Your Own Device Policies

Collection of Slack and Teams

Mobile Device Collections

Bring Your Own Device Policies

Since many companies and firms will be continuing to work remotely for the foreseeable future, now is a good time to either re-create, review, or revise your Bring Your Own Device policy. Historically, BYOD dealt principally with cell phones in order to avoid requiring employees to carry both a business and a personal cell phone. Now, BYOD is more about managing the flow of company data to personal devices or cloud storage.

The primary risk in using a personal computer to do corporate work is leaving documents or traces of data on the personal computer such that the data is outside of the control of the company. If the company has Virtual Private Network (VPN) technology, using a personal computer as a portal to log in to that VPN presents a low risk of company data transfer. In this scenario, IT administrators have many opportunities to mitigate security risks since data resides on corporate assets. For example, disabling the ability of remote desktop clients to connect to hard drives or using the copy/paste function prevents the user from inadvertently copying and pasting data between their work and personal computers. The BYOD policy should specifically address what happens if corporate data does end up on personal computers and what remedies should be made to remove that data.

However, if employees are using their personal computers, cellphones, or tablets to store or process company data, other precautions must be put in place such as encryption, segregation of data, and strong passwords. BYOD policies would need to include procedures that check and enforce these security measures. It is inadvisable to allow this since personal devices may be multi-user (and not all users are employees), backup procedures may not be sufficient, and there is a chance corporate data may be copied to the cloud during an automatic syncing event (such as Apple iCloud or OneDrive).

Collection of Slack and Teams

Collaboration software is proving indispensable during this time of remote work. Along with the convenience of working on projects with co-workers comes increased security risks as well as eDiscovery complications should that data be necessary to collect for litigation.

With Slack, data is stored in the cloud so companies and firms should carefully consider whether cloud storage is acceptable for their information. When using Slack, users are generally a part of a channel and can make posts and comments. It is similar to Facebook in that users can create a post, add attachments, edit, and delete posts. Other Slack users can see editing has occurred and they may still be able to see the original post. Administrators with certain privileges can generally recover previous versions and edits. Administrative users can download a Slack archive; unfortunately, the data does not lend itself to easy conversion to eDiscovery formats such as CSV files. This may mean using a vendor with expertise in handling this type of data if Slack data is needed in litigation.

Files that are shared on Teams are stored in a SharePoint folder and those shared in a private or group chat are stored in the OneDrive folder. Depending on how a company or firm has deployed Team, this means the data can be on premises or in the cloud, so that security risk depends on how it is installed. Teams does not provide tools for document management, but Sharepoint may have some file history information. Since Microsoft Teams

is more tightly integrated with their Exchange and Sharepoint platforms, there are a variety of eDiscovery functions available through the management console such as searching, litigation holds, and export of data. Once exported, the data can go through a typical eDiscovery process.

Mobile Device Collections

Knowing what is possible to collect from mobile devices can help inform BYOD policies. The actual collection of mobile devices has gotten both easier and harder depending on the type of device and its configuration. In general, investigations of cell phones are looking for text messages, location information, power-on events, and pictures.

Forensic data collection will collect the data on the device and not necessarily what the device can access. Therefore, BYOD policies should contemplate the additional collection of information from online backups or corporate mail servers. Note that downloaded files and draft or unsent email messages may be present on the actual device. There is a possibility that full file system collections may be possible for certain types of iPhones, called Checkm8; a full file system collection retrieves more information than the typical logical extraction, including full emails and third party application information.

Text messages are an area of interest during forensic collections that should be addressed in any BYOD policy. In general, the text messages are stored on the device of the sender and receiver and but not by the network that transmitted the data. Note that some text message services (such as Apple streaming) delivers a text message to every device that is configured to receive messages from the stream. This may also be true for Android devices, as well as chat apps such as WhatsApp. The implication is that non-corporate users could have access to those messages or data without the sender's knowledge.