CSO

FEATURE

Seductive technology: What are its implications for data security?

Alluring devices like the Apple iPhone have caused a shift towards the "Bring Your Own Device" paradigm, but what does it mean for both personal and corporate security?

By Ronald Kaplan and Dylan Kaplan

CSO | Sep 4, 2013 8:00 AM PT

The seduction of equipment designed by visionaries at companies like Apple, BlackBerry, Google, HP and Samsung has resulted in some unanticipated consequences. Traditionally, all devices in the corporate environment used to send or receive email, text messages or any other written business correspondence have been under the control of the Information Technology (IT) department. IT reviewed, tested, managed and authorized all devices and software used to send and receive information by company employees.

While companies like BlackBerry (formally known as Research In Motion) found their way into corporate use by appealing to the security and vulnerability sensibilities of IT decision makers, the iPhone, however, was not designed to seduce IT management. Instead, its elegance was designed to seduce everyone else, including corporate executives. And it did.

Many industry watchers identify the iPhone as the catalyst for the acceptance of equipment designed for the personal mobile market by the corporate user. Once executives realized these new, elegant and powerful devices could also be used for corporate communications, they demanded that IT enable them to replace their mobile devices with the iPhone. This opened the door for all levels of employees to use both iPhones and other smartphones to send, receive and store corporate information in addition to personal data. This was where design, ease of use, and the uncontrollable power of corporate executives won out over the objections of those charged with securing and managing corporate data; employees began to integrate their personal devices in a business setting. This became known as "Bring Your Own Device" (BYOD). As the need for BYOD policies were forced on IT departments around the globe, the line partitioning personal and work data started to blur.

[What's wrong with this picture? The NEW clean desk test]

What is the significance of the BYOD shift? Why is it important that the gatekeepers lost control of the gates? How does this affect individuals and corporations?

One needs look no further than the trial of Conrad Murray, the doctor convicted in the death of Michael Jackson, to gain insight into these questions. Dr. Murray had an iPhone and used it for both personal and work purposes while caring for Jackson, even at times when Jackson was under distress.

Both the personal and business evidence found on Murray's iPhone were examined and used to impugn his statements at trial by a computer forensics expert and went virtually unchallenged. However, much of the other evidence was, and continues to be, challenged or subjected to multiple interpretations.

Electronic data is very powerful evidence. It is often unfiltered and contemporaneous. Electronic forensic data can be challenged, but if properly examined, documented, analyzed and presented, attempts are usually unsuccessful. This data is time and date stamped and carries the signature of its author. Despite the fact that smartphones continuously record and store what may turn out to be a "smoking gun," users still embrace it. The seduction of these convenient and powerful tools has made them irresistible. Even those who are aware of the potential hazards of these devices' perfect memory continue to use them with callous disregard.

While working at SICons, a computer forensics firm, we observed firsthand the full range of data that can be found on all types of digital media. We witnessed multiple cases that relied on discovered electronic data, some obvious and straightforward, while others required reconstruction and interpretation of disjointed data.

Many people who use smartphones are aware that they can be lost, stolen, used to track their movements, likes and dislikes, use of slang, hobbies, and propensities. Despite their realization of the trail captured on these devices, many will likely leave a discoverable record of activities they would not want others to have or see. This is irrational, but true.

History has shown the power of seduction, in other forms, like the take down of politicians like Eliot Spitzer and Mark Sanford, but being taken down by your own smartphone is different. In Spitzer- and Sanford-type cases, the subject is aware of the need to operate in secrecy and usually takes appropriate precautions. In these cases, your guard is up and you know that you have to be careful. However, the smartphone is your friend and confidant; you take it everywhere and keep no secrets. It has unimpeachable memory and therefore no "he said, she said" disputes can ensue.

We have no *solutions* to offer to those who commingle personal and corporate data and thus subject devices to discovery in civil and criminal matters. What we do have is advice for those who use digital communication devices for confidential personal and business data: exercise caution, as the evidence on your device, on the devices of those you communicated with, and on intermediary devices is often exposable. Even innocent actions can be carved from the data found on these devices, taken out of context and used to imply guilt.

Just like the ubiquitous video camera, now spread all over the planet and capturing all types of activities that used to go undocumented (this was evident in the capture of the Boston Marathon terrorists), so too do these portable devices expose secrets and provide indisputable evidence. As we recognize that personal computers, smartphones and tablets are the "bicycle for the mind," it becomes evident why we choose to bike, even at times when it would be most prudent to walk.

For decades, IT departments have moved in the direction of standardization and centralization to implement data security solutions. Clearly, these seductive devices have put IT infrastructure and control in jeopardy. IT's loss of control can have far-reaching implications from the perspective of information security.

Information that has been created can find its way to the most inopportune and undesirable destinations, unless the lifecycle of that information, from creation to destruction, is carefully managed. Rather than fighting to defend IT's boundaries against device indifference, corporate America should embrace the new paradigm and insist that IT's interests be incorporated into the devices.

Mr. Ronald Kaplan, MS, MBA is a partner at SICons, a management consulting and computer forensic expert witness firm in Los Angeles. Dylan Kaplan, BS, is a recent graduate of the Eller College of Management at the University of Arizona, specializing in Management Information Systems. While at the University of Arizona, Dylan worked at Apple Inc. providing technical support.