PUBLICATION

Eight Keys to Securing Portable Devices

Authors: Zachary B. Busey
March 10, 2017

Securing physical worksites and workspaces is by now old hat. We all know file cabinets should be locked, worksites secured and personal access to information monitored. Securing portable devices, however, often receives less attention. We assume our phone is secure because it is in our pocket, or our laptop can't be hacked because it is inside of a locked car or in your house. These assumptions can be costly. Here are eight keys to help you secure portable devices.

1. Encryption

As encryption tools become more and more accessible, encryption should be considered the default when it comes to protecting confidential or sensitive information. Information should be encrypted both upon transmittal and at rest. Thus, not only should a laptop's hard drive be encrypted, but so should sensitive files and information that may be sent or transmitted from the laptop. Most laptops, phones and other portable devices have some form of default or native encryption. For more advanced encryption options, third-party and after-market options are available.

2. Passwords and Multi-Factor Authentication

Encryption may be thwarted if the access key or password is easily deciphered. While many view passwords as an inconvenience – especially password requirements: upper case letter, number and a symbol – a password's importance cannot be overstated. Passwords – and, yes, minimum password requirements – should be mandatory for all portable devices, as well as any virtual access point to company documents or information. In addition, users should be required to change their passwords frequently, and they should be restricted from using consecutive iterations of the same password (e.g., "Password001," "Password002," etc.). Users should also be restricted from sharing their passwords or leaving them on sticky notes affixed to the back of their laptop or computer monitor. In most instances, companies should strongly consider multi-factor authentication or MFA. MFA requires something in addition to a password, like a fingerprint, phone call or additional passcode generated from another source. For sensitive information, such as health information, financial information or customer data, MFA should be required.

3. Control Access

Passwords and encryption restrict access to authorized users. Companies also want to restrict access among authorized users. This is most easily described with reference to a familiar setting: the file room. Although every employee is allowed access to the building, not every employee is allowed access to the file room (or the vault, or certain workspaces, etc.). Electronically stored information should be treated the same way, and access from portable devices should be restricted. Additionally, access logs should be created and monitored regularly. In the event of internal unauthorized access, the appropriate corrective action should be taken. Companies likewise should be diligent in correcting the system flaw so as to avoid future instances of unauthorized access.

4. Backups

Bad things happen and will always happen at the most inconvenient time. Backups and restoration protocols help limit the fallout when things go wrong. Whether it is a lost laptop or corrupted portable drive, a backup can literally save the day. However, be careful not to sacrifice security for convenience. Backups should be treated

no differently than the original data and they should be encrypted and password protected. Duplicating information can be an important lifeline. However for every copy that is made, that is one more copy for which a company must account. To ease this burden, backups should be routinely and securely deleted – consistent with a company's document and information retention policies.

5. Updates

Updates and patches are the unsung heroes of the portable device world. Staying up-to-date on the latest in viruses, backdoors and malware can be overwhelming. Fortunately, almost every company that makes a portable device issues updates and patches. Left uninstalled, these updates and patches are no better than a sticky note titled "important passwords." As with routine destruction of backups, companies must ensure that updates and patches are installed regularly. Portable devices should be regularly inventoried, and those without the latest updates and patches should be revoked from a company's network or virtual points of access.

6. Mobile Device Management

As the name implies, mobile device management (or MDM) is a broad category of software and applications that help secure portable devices – mostly laptops, tablets and phones. MDM can allow phones to be remotely controlled or wiped. It can set minimum security requirements for any portable device, and, for example, it can be used on laptops or other computers to require any external device or drive to be password protected. MDMs vary greatly and how it should be used by your company will depend on your company's specific needs and technological capabilities.

7. Be Smart when Using Your Devices

Being smart about how and when confidential business information is accessed goes a long way. For instance, the free Wi-Fi at a hotel or local coffee shop is not secure and should be avoided when accessing confidential information. Further, mobile device applications should only be installed from a trusted source. Moreover, users should be selective about granting permission for a third-party to access their mobile devices, such as granting Google maps access to track a user's location. Finally, a mobile device's security settings should not be altered.

8. Written Policies

Written policies tie together all of the above. They should make clear what is permitted and what is not. They should also cover less obvious areas like privacy and liability. Written policies should disclaim any liability for damage to employee-provided devices, or the loss/corruption of data on employee-provided devices. The policies should also make clear that there is no right to privacy on any portable device that accesses a company's networks or information. Any individual using a portable device to access company information should receive a copy of the applicable written policies and execute a verification or acknowledgment.

These tips are now the new normal when it comes to securing portable devices. Some are easier to implement than others, but all are important to protecting confidential or sensitive information. If you have any questions, please contact the authors of this alert – Zachary B. Busey and Mindy L. Rattan – or any member of the Firm's Data Protection, Privacy and Cybersecurity Team.